

特許協力条約

E P

U S

P C T

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

| | | |
|---------------------------------|---------------------------------------------------------|----------------|
| 出願人又は代理人 の書類記号 520269W001 | 今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。 | |
| 国際出願番号 PCT/JPO/00474 | 国際出願日 (日.月.年) 28.01.00 | 優先日 (日.月.年) |
| 出願人(氏名又は名称) 三菱電機株式会社 | | |

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
 この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
 この国際出願に含まれる書面による配列表

この国際出願と共に提出されたフレキシブルディスクによる配列表

出願後に、この国際調査機関に提出された書面による配列表

出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. 請求の範囲の一部の調査ができない(第I欄参照)。

3. 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は 出願人が提出したものを承認する。

次に示すように国際調査機関が作成した。

5. 要約は

出願人が提出したものを承認する。

第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1ヶ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 2 図とする。 出願人が示したとおりである。

なし

出願人は図を示さなかった。

本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl'

H 04 L 9/08

H 04 L 29/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl'

G 09 C 1/00 - 5/00

H 04 L 9/00

H 04 K 1/00 - 3/00

H 04 L 29/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

INSPEC (DIALOG)

C. 関連すると認められる文献

| 引用文献の カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する 請求の範囲の番号 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|------------------|
| Y | Paul Albits and Cricket Liu, 高田広章, 小島育夫監訳, 小舘光正訳, 「DNS & BIND 第3版」第2版, オライリー・ジャパン, (1999年6月3日), pp. vii-ix, 100-102 | 1-12 |
| Y | RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions," (Jan 1997) | 1-12 |
| A | RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," (Nov 1987) | 1-12 |

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

| | |
|-------------------------------------------------------------------------|-------------------------------------------------------------------|
| 国際調査を完了した日 13.04.00 | 国際調査報告の発送日 25.04.00 |
| 国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号 | 特許庁審査官 (権限のある職員) 丸山 高政 5W 9570 電話番号 03-3581-1101 内線 9570 |

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年8月2日 (02.08.2001)

PCT

(10) 国際公開番号
WO 01/56223 A1

(51) 国際特許分類7: H04L 9/08, 29/02

[JP/JP]. 足立一幸 (ADACHI, Kazuyuki) [JP/JP]. 篠田誠一 (SHINODA, Seiichi) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

(21) 国際出願番号: PCT/JP00/00474

(74) 代理人: 溝井章司, 外 (MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).

(22) 国際出願日: 2000年1月28日 (28.01.2000)

(81) 指定国 (国内): CA, IL, JP, US.

(25) 国際出願の言語: 日本語

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).

(85) 添付公開書類:
— 国際調査報告書

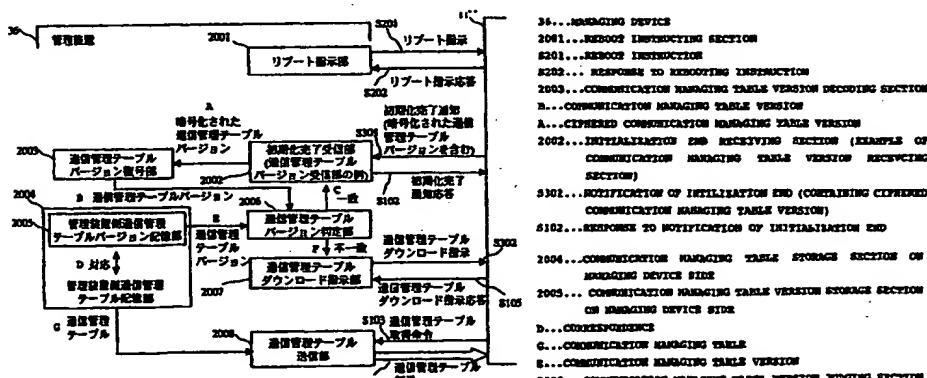
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 武田紀子 (TAKEDA, Noriko) [JP/JP]; 〒100-0006 東京都千代田区有楽町一丁目12番1号 三菱電機システムウエア株式会社内 Tokyo (JP). 笹本明彦 (SASAMOTO, Akihiko)

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

(54) Title: COMMUNICATION MANAGING TABLE TRANSFER SYSTEM AND MANAGING DEVICE, CIPHERING DEVICE, AND COMMUNICATION MANAGING TABLE TRANSFER METHOD

(54) 発明の名称: 通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法



WO 01/56223 A1

(57) Abstract: A communication managing table transfer system comprising ciphering devices interconnected through an internet, a managing device for managing a communication managing table used for communication by the ciphering devices, providing improved security, and having improved performance. A managing device (36) receives a communication managing table version from a ciphering device (11) (S301), a communication managing table version judging section

/締書有り



(2006) compares the received communication table version with the communication managing table version stored in a communication managing table version storage section (2005) on the managing device side and transfers the communication managing table to the cipher device (11) only if the result of the comparison shows that both disagree with each other (S104).

(57) 要約:

インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置となる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上とを図ることを課題とする。

管理装置 3 6 は、暗号装置 1 1 から通信管理テーブルバージョンを受信し (S 3 0 1)、通信管理テーブルバージョン判定部 2 0 0 6 で、管理装置側通信管理テーブルバージョン記憶部 2 0 0 5 に記憶している通信管理テーブルバージョンと比較し、不一致の場合にのみ暗号装置 1 1 に対して通信管理テーブルを転送する (S 1 0 4)。

明細書

通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法

5

技術分野

本発明は、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上に関する。

背景技術

近年、仮想私設網（VPN: Virtual Private Network）を用いるシステムが普及している。仮想私設網は、データの暗号化やユーザ認証などのセキュリティ技術を用いてインターネット等のパブリックネットワークを仮想的（Virtual）に専用線（Private Network）のように利用するネットワークのことである。仮想私設網によって、複数の組織における内部ネットワーク間を専用線を用いるかのごとく接続することができる。

20 図13は、仮想私設網を用いるシステムの例を示す図である。1は、インターネット、11、21、31は、暗号装置、12、22、32は、ルータ、13、23、33は、ファイアウォール、14、24、34は、サブネット（内部ネットワーク）、15、25、35は、通信端末、36は、管理装置である。それぞれ、図のように接続されている。

25 インターネットを介したデータ転送を行なう場合、外部からの攻撃に対する防御手段としてIP securityに準拠するシステムが用

いられる。IP securityは、インターネット通信規約標準化機関IETF (Internet Engineering Task Force) で定められたIPパケットレベルにおけるセキュリティ確保方式のことである。

5 IP securityでは、各内部ネットワーク上の暗号装置間で、SA (Security Association) という関係を確立した上で、データの転送を行なう。これにより、秘匿通信が可能となる。しかし、SAを確立する為には、その前提として公開鍵を暗号装置間で共有化しておく必要がある。

10 また、内部ネットワーク上の通信端末に対してデータを転送する場合には、各内部ネットワークの構成情報を知っておく必要もある。

そのため、上記の公開鍵や内部ネットワークの構成情報を含む通信管理テーブルを生成し、SAの確立の前にこの通信管理テーブルを暗号装置間で交換する。このような通信管理テーブルを作成し、更新し、配信するために管理装置36が設置される。

従来、暗号装置から通信管理テーブルを求められた管理装置36は、無条件に通信管理テーブルを暗号装置へ配信していた。

20 図14は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。暗号装置A11の電源がいれられると、暗号装置A11は、暗号装置初期化通知 (S101) を送信する。管理装置36は、暗号装置初期化通知 (S101) を受信すると、暗号装置初期化通知応答 (S102) を送信する。暗号装置A11は、暗号装置初期化通知応答 (S102) を受信すると無条件に通信管理テーブル取得命令 (S103) を発行し、通信管理テーブル転送 (S104) が行なわれる。

また、図15は、従来例におけるリポートされたときの通信管理テー

ブルの転送の手順を示す図である。管理装置 3 6 が、リブート指示 (S 2 0 1) を送信し、暗号装置 A 1 1 が、リブート指示応答 (S 2 0 2) を送信した後、再起動する。これ以降、図 1 4 と同様に動作する。

5 上述のシステムにおいては、通信管理テーブルの転送回数が多く、データ転送の性能を劣化させていた。

また、通信管理テーブルを盗用される機会を増加させ、セキュリティ上の問題があった。つまり、公開鍵や内部ネットワークの構成情報を盗まれ、暗号装置間のデータ転送の秘匿が守られないおそれがあった。

10 本発明は、上記した従来技術の欠点を除くためになされたものであって、通信管理テーブルの転送回数を減らし、データ転送の性能を向上させ、通信管理テーブルを盗用される機会を減らし、セキュリティを向上させることを目的とする。

発明の開示

15 この発明に係る通信管理テーブル転送システムは、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

20 上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

25 上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージ

ジョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする。

この発明に係る管理装置は、インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする。

この発明に係る暗号装置は、インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

10 上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

15 上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

25 上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶する

ことを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする。

上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする。

この発明に係る通信管理テーブル転送方法は、インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信

管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

5 上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

10 上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

15 上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする。

図面の簡単な説明

図1は、本実施例における暗号装置の構成を示す図である。

20 図2は、本実施例における管理装置の構成を示す図である。

図3は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図4は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。

25 図5は、本実施例におけるリポートされたときの通信管理テーブルの転送の手順を示す図である。

図 6 は、本実施例におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。

図 7 は、本実施例における通信管理テーブルの構成を示す図である。

図 8 は、本実施例における通信管理テーブルの構成を示す図である。

5 図 9 は、本実施例における通信管理テーブルの構成を示す図である。

図 10 は、SA確立の際のデータフローを示す図である。

図 11 は、秘匿通信の際のデータフローを示す図である。

図 12 は、サブネット構成情報の使用例を示す図である。

図 13 は、仮想私設網を用いるシステムの例を示す図である。

10 図 14 は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図 15 は、従来例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

15 発明を実施するための最良の形態

実施の形態 1.

以下、本発明を図面に示す実施例に基づいて説明する。

図 1 は、本実施例における暗号装置の構成を示す図である。1001 は、電源制御部、1002 は、リブート制御部、1003 は、初期化部、1004 は、暗号装置側通信管理テーブル記憶部、1005 は、暗号装置側通信管理テーブルバージョン記憶部、1006 は、通信管理テーブルバージョン暗号化部、1007 は、初期化完了通知部、1008 は、通信管理テーブルダウンロード制御部、1009 は、通信管理テーブル受信部である。

25 図 2 は、本実施例における管理装置の構成を示す図である。2001 は、リブート指示部、2002 は、初期化完了受信部、2003 は、通

信管理テーブルバージョン復号部、2004は、管理装置側通信管理テーブル記憶部、2005は、管理装置側通信管理テーブルバージョン記憶部、2006は、通信管理テーブルバージョン判定部、2007は、通信管理テーブルダウンロード指示部、2008は、通信管理テーブル送信部である。

図3は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。以下、この手順について、図1及び図2の構成に基づいて説明する。

暗号装置A11側では、電源を入れられると、電源制御部1001が初期化部1003に初期化を指示する。初期化部1003は、初期化を完了すると初期化完了通知部1007に初期化の完了を知らせる。初期化完了通知部1007は、管理装置36の初期化完了受信部2002に暗号装置初期化完了通知(S301)を送信する。このとき管理装置36の公開鍵により暗号化した通信管理テーブルバージョンが、暗号装置初期化完了通知(S301)に含まれている。

通信管理テーブルバージョンは、暗号装置側通信管理テーブルバージョン記憶部1005に記憶されている。暗号装置側通信管理テーブルバージョン記憶部1005の通信管理テーブルバージョンは、暗号装置側通信管理テーブル記憶部1004の通信管理テーブルと対応付けられている。この例では、暗号装置側通信管理テーブルバージョン記憶部1005は、暗号装置側通信管理テーブル記憶部1004に含まれるが、別個に設けても構わない。

通信管理テーブルバージョン暗号化部1006は、暗号装置側通信管理テーブルバージョン記憶部1005から通信管理テーブルバージョンを読み、これを暗号化し、暗号化された通信管理テーブルバージョンを初期化完了通知部1007に送るように構成されている。

管理装置 36 側では、初期化完了受信部 2002 が、暗号装置初期化完了通知 (S301) を受信し、通信管理テーブルバージョン復号部 2003 が、暗号化されている通信管理テーブルバージョンを復号する。一方、通信管理テーブルバージョン判定部 2006 は、管理装置側通信管理テーブルバージョン記憶部 2005 から管理装置 36 側で記憶する通信管理テーブルバージョンを読む。そして、通信管理テーブルバージョン判定部 2006 は、これらの通信管理テーブルバージョンを比較する。尚、この実施例では、管理装置側通信管理テーブルバージョン記憶部 2005 は、管理装置側通信管理テーブル記憶部 2004 に含まれているが、通信管理テーブルと通信管理テーブルバージョンが対応付けられていれば、別個に設けても構わない。

比較の結果、2つの通信管理テーブルバージョンが不一致の場合には、通信管理テーブルバージョン判定部 2006 は、通信管理テーブルダウンロード指示部 2007 に不一致を知らせる。

通信管理テーブルダウンロード指示部 2007 は、不一致の知らせを受けると、暗号装置 A11 の通信管理テーブルダウンロード制御部 1008 に通信管理テーブルダウンロード指示 (S302) を送信する。

暗号装置 A11 側では、通信管理テーブルダウンロード制御部 1008 が、通信管理テーブルダウンロード指示 (S302) を受信するとファイル転送の手順に従って通信管理テーブルを受信する為に、通信管理テーブル受信部 1009 に通信管理テーブル取得の指示を送る。

通信管理テーブル受信部 1009 は、その指示を受けると、管理装置 36 の通信管理テーブル送信部 2008 に通信管理テーブル取得命令 (S103) を送る。

管理装置 36 側では、通信管理テーブル取得命令 (S103) を受けた通信管理テーブル送信部 2008 は、管理装置側通信管理テーブル記

憶部 2004 から通信管理テーブルを読み、その通信管理テーブルを暗号装置 A11 の通信管理テーブル受信部 1009 にファイル転送する (S104)。

暗号装置 A11 側では、通信管理テーブル受信部 1009 が通信管理テーブルを受信し終えると、通信管理テーブルダウンロード制御部 1008 に通信管理テーブル取得の完了を知らせ、通信管理テーブルダウンロード制御部 1008 は通信管理テーブルダウンロード指示応答 (S105) を管理装置 36 の通信管理テーブルダウンロード指示部 2007 に送信する。また、通信管理テーブル受信部 1009 は、受信した通信管理テーブルを暗号装置側通信管理テーブル記憶部 1004 に記憶する。

この例では、ファイル転送のときに通信管理テーブルに通信管理テーブルバージョンを含めて転送し、暗号装置側通信管理テーブル記憶部 1004 は通信管理テーブルバージョンを含む通信管理テーブル記憶している。しかし、通信管理テーブルバージョンを、通信管理テーブルに含めない構成にすることもできる。つまり、通信管理テーブルバージョンを含まない通信管理テーブルと、通信管理テーブルバージョンを別個にファイル転送することも可能である。

このようにして、通信管理テーブルバージョンが一致しない場合は、通信管理テーブルが管理装置 36 から暗号装置 A11 へ転送される。また、通信管理テーブルバージョンも転送される。

図 4 は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。以下、この手順について、図 1 及び図 2 の構成に基づいて説明する。

通信管理テーブルバージョン判定部 2006 が、通信管理テーブルバージョンを比較するまでの手順は、上述の手順と同様である。

比較の結果、通信管理テーブルバージョンが一致した場合には、通信管理テーブルバージョン判定部 2006 は、一致を初期化完了受信部 2002 に知らせる。

初期化完了受信部 2002 は、暗号装置初期化完了通知応答 (S105.2) を初期化完了通知部 1007 に送信する。初期化完了通知部 1007 が、暗号装置初期化完了通知応答 (S102) を受け取ると動作を終了する。つまり、通信管理テーブルバージョンが一致する場合は、通信管理テーブルの転送は行なわれない。

暗号装置 A11 が通信管理テーブルバージョンを送信し、管理装置 310 6 が通信管理テーブルバージョンを判定するタイミングは、初期化の時に限られない。システムで自由に設定することができる。例えば、リブートのタイミングや、定期的なタイミングであっても構わない。

図 5 は、本実施におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。また、図 6 は、本実施におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。リブート指示 (S201) とリブート指示応答 (S202) に基づく再起動から始まる点を除き、図 3 及び図 4 の手順と同様である。

次に、通信管理テーブルの構成について説明する。図 7、図 8 及び図 9 は本実施例における通信管理テーブルの構成を示す図である。

20 通信管理テーブルには、通信管理テーブルバージョン 90 のほか、インターネット通信用情報 A50、インターネット通信用情報 B60 等のインターネット通信用情報と、サブネット構成情報 A70、サブネット構成情報 B80 等のサブネット構成情報が含まれる。

25 インターネット通信用情報 A50 は、暗号装置 A11 がインターネット 1 を介して、他の暗号装置と通信する場合に必要になる情報である。インターネット通信用情報 B60 も同様に、暗号装置 B21 がインター

ネット 1 を介して、他の暗号装置と通信する場合に必要になる情報である。

5 1、6 1は、インターネットアドレス、5 2、6 2は、暗号装置の識別子、5 3、6 3は、認証書、5 4、6 4は有効期限である。認証書

5 には、S A用公開鍵が含まれている。

サブネット構成情報A 7 0は、サブネット1 4の構成に関する情報である。この図では、1 レコードのみ示しているが、サブネット1 4の構成に含まれる通信端末が多い場合には、更にレコードが付加されている。サブネット構成情報B 8 0も同様である。

10 7 1、8 1は、暗号装置の識別子、7 2、8 2は、ネットワークアドレス、7 3、8 3は、ネットマスクである。

図7の例では、通信管理テーブルバージョン9 0は、バージョンは一つであり、通信管理テーブル全体の更新状況に対応している。

15 図8の例では、通信管理テーブルバージョン9 0は、暗号装置A情報バージョン9 1、暗号装置B情報バージョン9 2等複数のバージョンから構成されている。暗号装置A情報バージョン9 1は、インターネット通信用情報A 5 0とサブネット構成情報A 7 0等（サブネット構成情報A 7 0の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

20 図9の例では、更に細分化し、通信管理テーブルバージョン9 0は、暗号装置Aインターネット通信用情報バージョン9 3、暗号装置Aサブネット構成情報バージョン9 4、暗号装置Bインターネット通信用情報バージョン9 5、暗号装置Bサブネット構成情報バージョン9 6等のバージョンから構成されている。暗号装置Aインターネット通信用情報バージョン9 3は、インターネット通信用情報A 5 0の更新状況に対応している。また、暗号装置Aサブネット構成情報バージョン9 4は、サブ

ネット構成情報A70等（サブネット構成情報A70の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図8と図9の場合に、バージョンと各情報との対応をつけるために、各バージョンに対応して装置識別子や情報識別子を記憶する方法も考えられる。

管理装置36は、各暗号装置から、通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部（図示せず）と、管理装置側通信管理テーブルと、管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部（図示せず）を有する。

図7の場合、通信管理テーブル更新情報受信部は、いずれの暗号装置から通信管理テーブル更新情報を受信した場合にも、通信管理テーブルバージョン90を更新する。図8の場合、通信管理テーブル更新情報受信部は、暗号装置A11から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報A50、サブネット構成情報A70のいずれか若しくは両方を更新し、更に暗号装置A情報バージョン91を更新する。図9の場合、通信管理テーブル更新情報受信部は、暗号装置A11から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報A50に関する通信管理テーブル更新情報、サブネット構成情報A70に関する通信管理テーブル更新情報のいずれか若しくは両方かを判断し、その部分を更新し、更にその部分に対応する暗号装置Aインターネット通信用情報バージョン93、暗号装置Aサブネット構成情報バージョン94のいずれか若しくは両方を更新する。

図8や図9のように、通信管理テーブルバージョンを細分化した場合には、通信管理テーブルバージョン判定部2006は、細分化したバージョン毎に比較し、通信管理テーブルのうち不一致のバージョンに関する

る部分のみを通信管理テーブル転送（S 1 0 4）で転送するようにすることも有効である。その場合は、通信管理テーブルダウンロード指示（S 3 0 2）に転送する部分を特定する情報を付加し、通信管理テーブル受信部 1 0 0 9 は、暗号装置側通信管理テーブル記憶部 1 0 0 4 の中の
5 その部分のみを更新し、暗号装置側通信管理テーブルバージョン記憶部 1 0 0 5 の中のその部分のバージョンのみを更新する。

次に、通信管理テーブルに含まれる S A 用公開鍵を用いて S A を確立する動作について説明する。図 1 0 は、S A 確立の際のデータフローを示す図である。この例では、暗号装置 A 1 1 が S A 確立を要求する側であり、暗号装置 B 2 1 が S A 確立の要求に応答する側である。それぞれの暗号装置は、自らの S A 用秘密鍵を記憶する S A 用秘密鍵記憶部 1 0 1 3 と、秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を共有化する秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 とを有する。秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、図に示すように、自らの S A 用秘密鍵と、相手側の S A 用公開鍵とを入力できるように構成されている。
10
15

暗号装置 A 1 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X a を生成し、署名し、暗号化し、暗号装置 B 2 1 側へ送信する（S 5 0 1）。暗号装置 B 2 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X b を生成し、乱数 X a と組合させて秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を生成する。更に、X b と X a のハッシュ値を署名し、暗号化し、暗号装置 A 1 1 側へ送信する（S 5 0 2）。暗号装置 A 1 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X a と乱数 X b とを組合させて秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を生成し、受信したハッシュ値を検証する。更に乱数 X b のハッシュ値を暗号装置 B 2 1 側に送信する（S 5 0 3）。暗号装置 B 2 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、受信したハッシュ値を検証す
20
25

る。以上の手順により、S Aが確立する。これによって、両者は、共通の秘匿信用秘密鍵1011と秘匿信用認証鍵1012を取得する。

次に、S A確立の後に行われる秘匿通信の動作について説明する。図11は、秘匿通信の際のデータフローを示す図である。この例では、暗号装置A11がデータを送信する側であり、暗号装置B21がデータを受信する側である。但し、S Aが確立している暗号装置間では、双方向の通信が可能であり、この例に限定されない。

それぞれの暗号装置は、インターネット通信部1014と、サブネット通信部1015とを有する。インターネット通信部1014は、インターネット1を介する通信を制御し、サブネット通信部1015は、サブネットを介する通信を制御する。

送信側のインターネット通信部1014は、暗号化部1016と、認証部1017と、エンカプセル処理部1018が動作する。また、受信側のインターネット通信部1014は、認証部1019と、復号部1020と、デカプセル処理部1021が動作する。この動作において、秘匿信用秘密鍵1011は、暗号アルゴリズムに使用され、秘匿信用認証鍵1012は、認証アルゴリズムに使用される。

また、通信管理テーブルに含まれるサブネット構成情報は、他の暗号装置に接続されるサブネットに対して通信を行なう場合に用いられる。図12に示すように、サブネット構成情報は、インターネット通信部1014で用いられる。

産業上の利用可能性

本発明においては、管理装置と暗号装置の間で、通信管理テーブルのバージョンを管理し、両者間の通信管理テーブルの同一性が確認できた場合には、通信管理テーブルの転送を行なわないように構成したので、

通信管理テーブルの転送回数が削減され、データ通信の性能及び安全性
が著しく向上する。

請求の範囲

1. インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

5 上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

10 上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

15 上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

20 上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

25 上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送

信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受

5 信部により受信された上記管理装置側通信管理テーブルを、上記暗号装
置側通信管理テーブルとして記憶することを特徴とする通信管理テーブ
ル転送システム。

2. 上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装
10 置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装
置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理
テーブル受信部により受信された上記管理装置側通信管理テーブルバ
15 バージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶する
ことを特徴とする請求項1記載の通信管理テーブル転送システム。

3. インターネットを介して互いに接続する複数の暗号装置
が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信
20 管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信
管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージ
25 ョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルで
ある暗号装置側通信管理テーブルのバージョンである暗号装置側通信管

理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

5 上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする管理装置。

4. 上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする請求項3記載の管理装置。

5. 上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする請求項3記載の管理装置。

6. 上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする請求項5記載の管理装置。

20 7. インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であつて、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信

管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

5 上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

10 上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする暗号装置。

8. 上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

15 上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項 7 記載の暗号装置。

9. 上記通信管理テーブルは、公開鍵を含み、

20 上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿通信用秘密鍵交換部を備えることを特徴とする請求項 7 記載の暗号装置。

10. 上記通信管理テーブルは、公開鍵を含み、

25 上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側

通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共に有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする請求項 7 記載の暗号装置。

11. 上記他の暗号装置は、サブネットに接続し、

5 上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴 10 とする請求項 7 記載の暗号装置。

12. インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

15 上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

20 上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

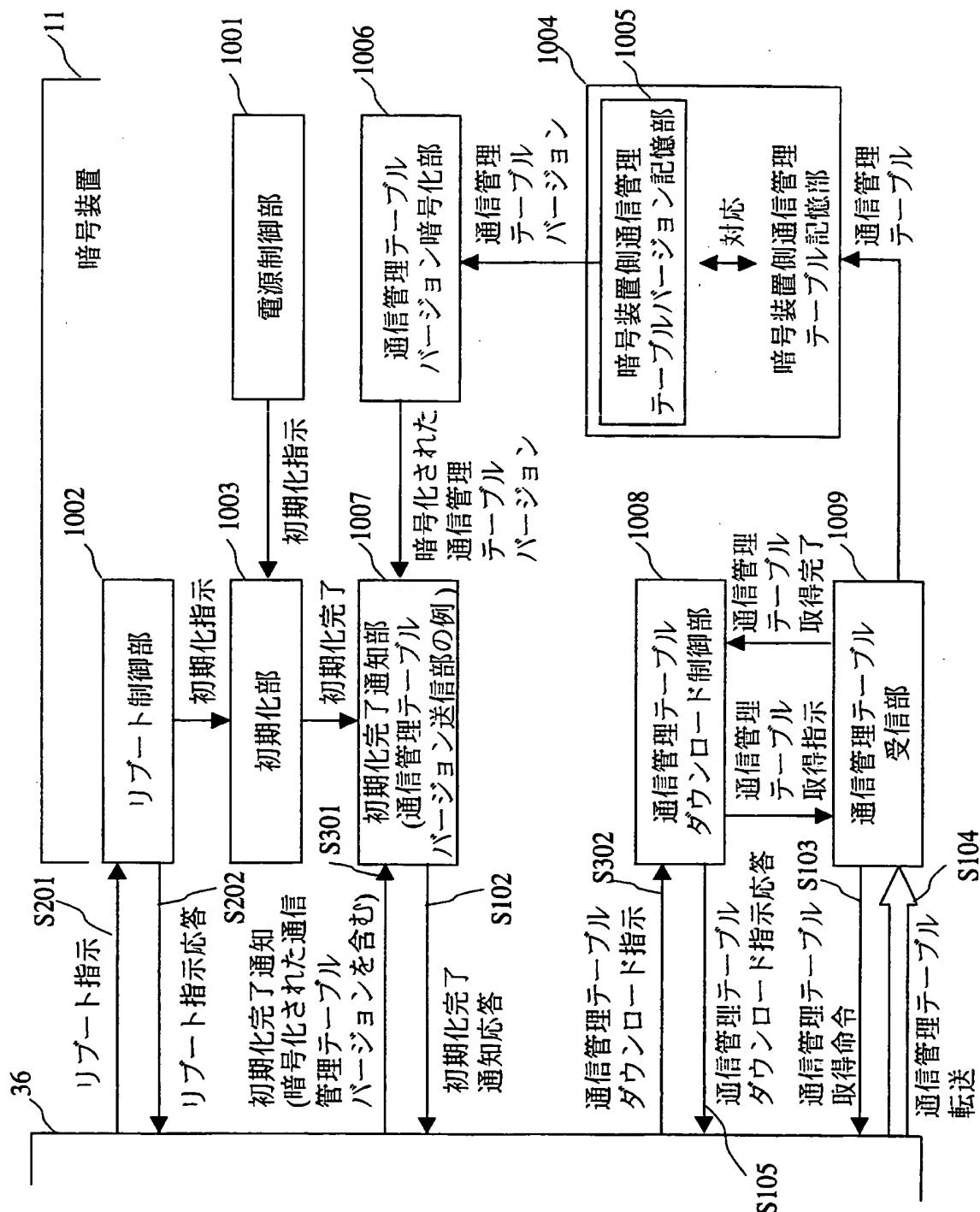
上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

- 5 上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする通信管理テーブル転送方法。

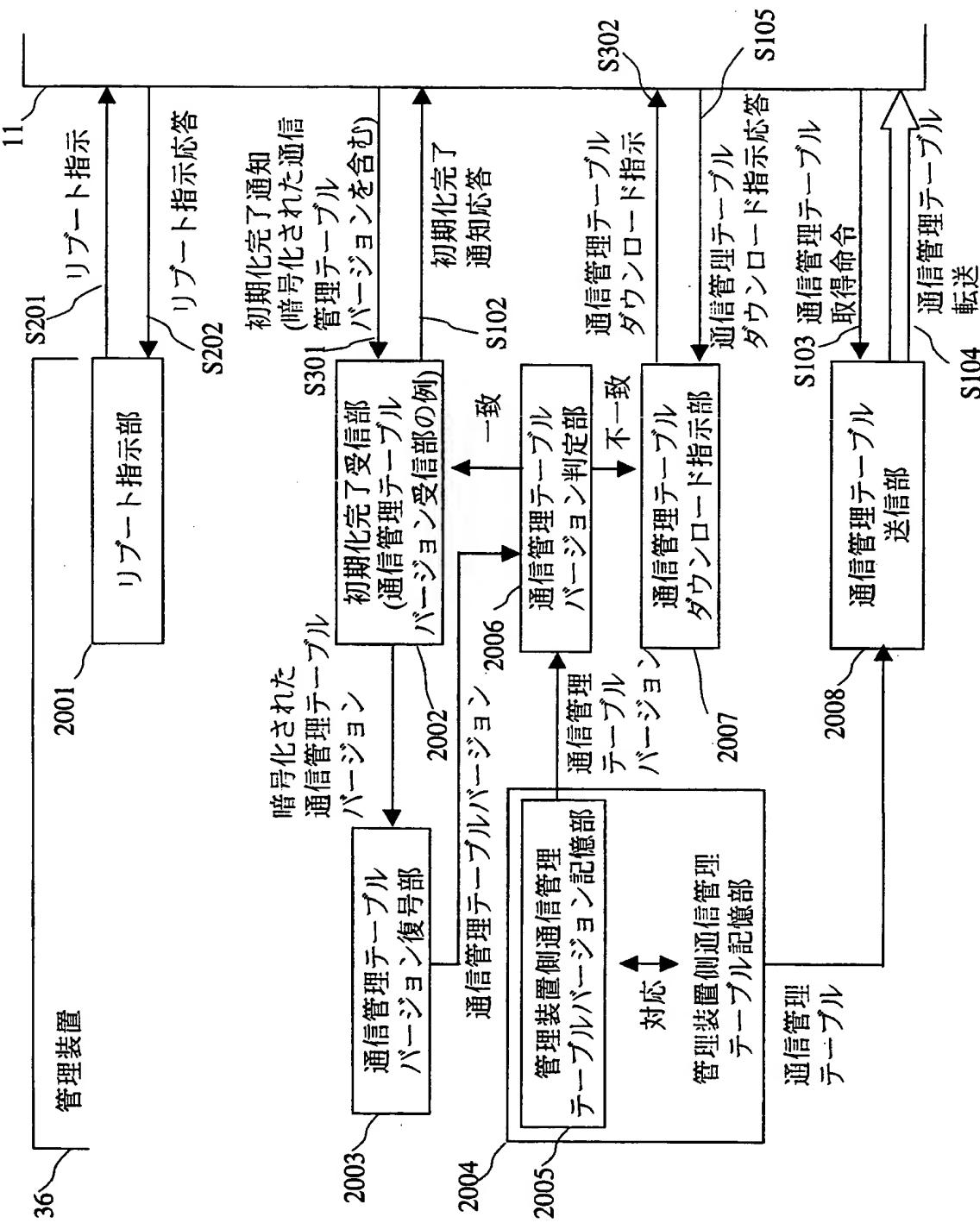
1/15

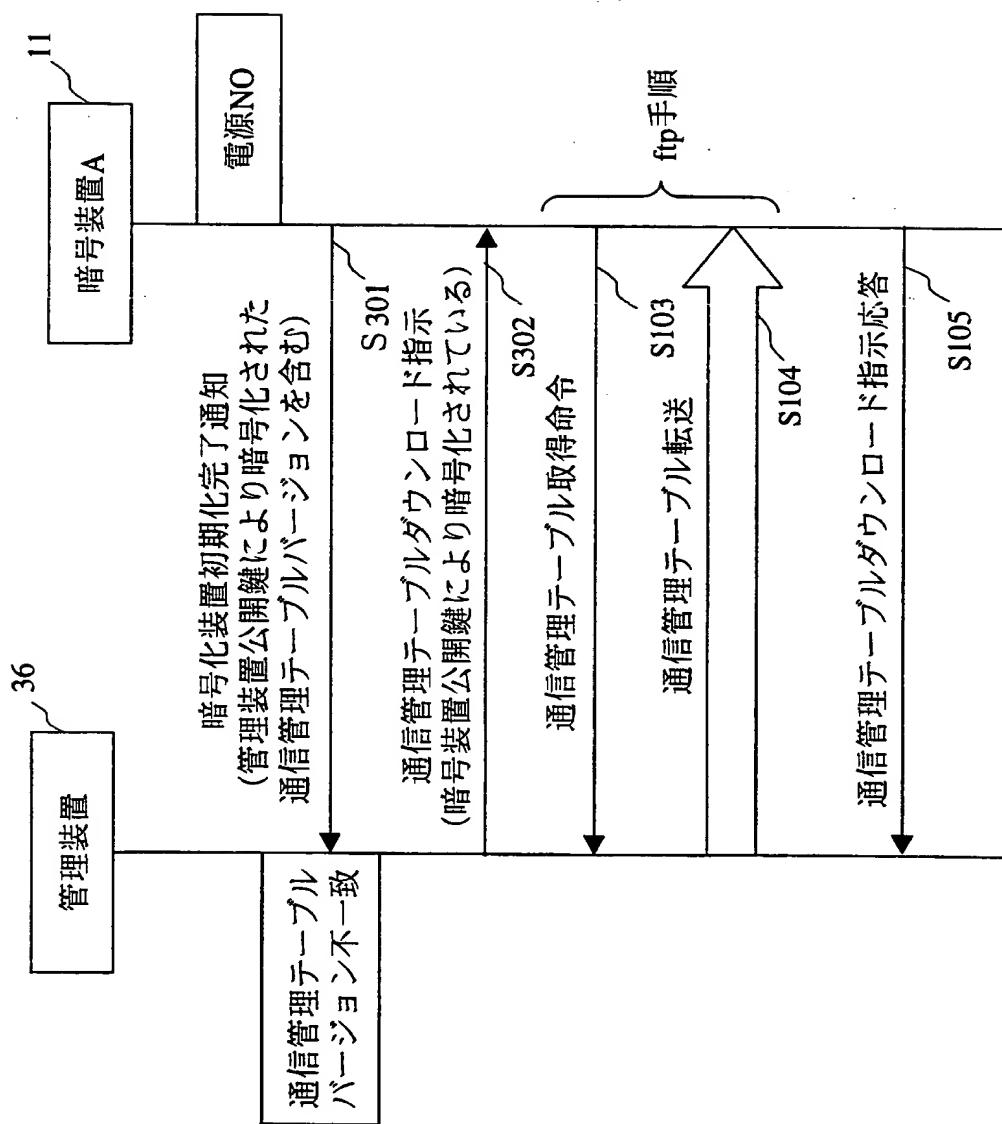
1



2/15

四 2

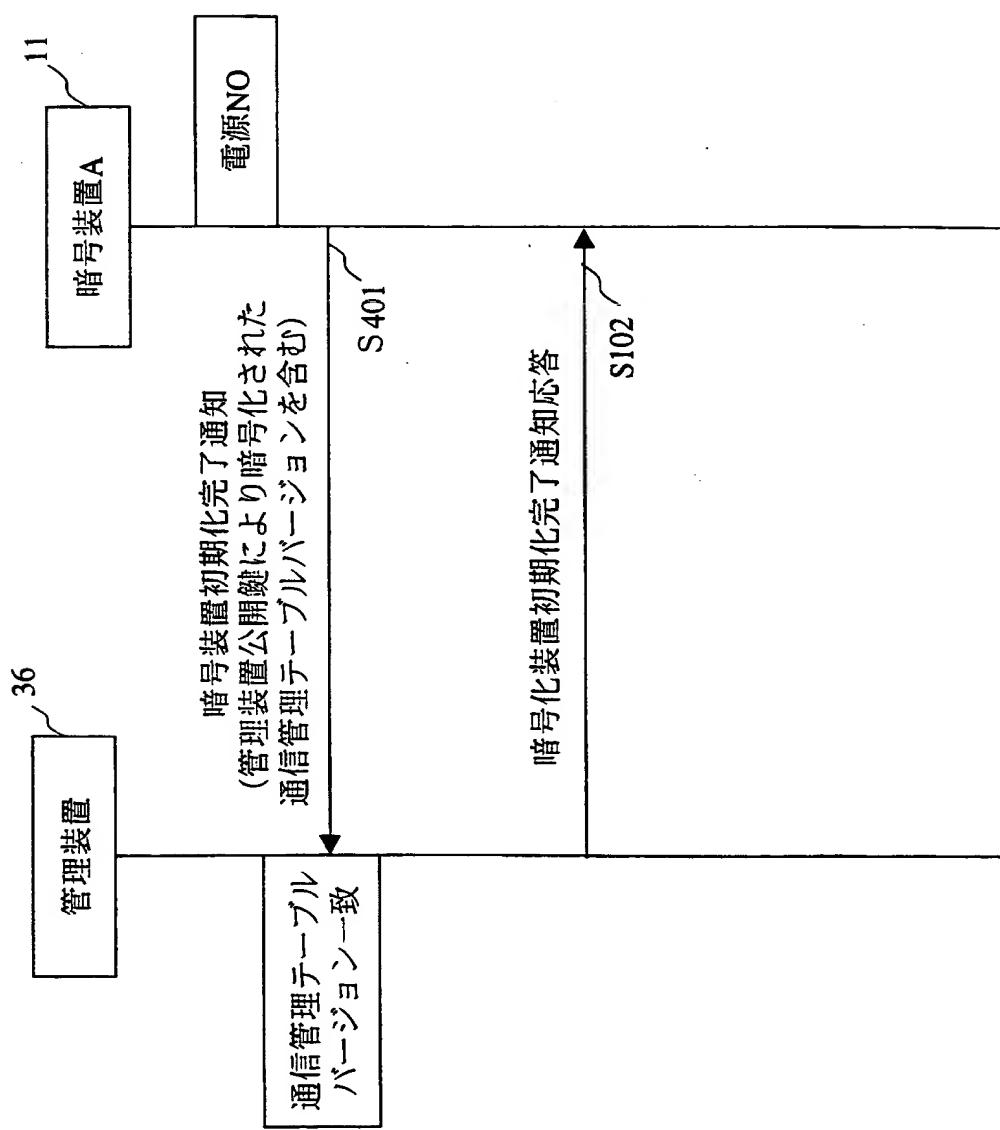


3/15
図3

4/15

☒

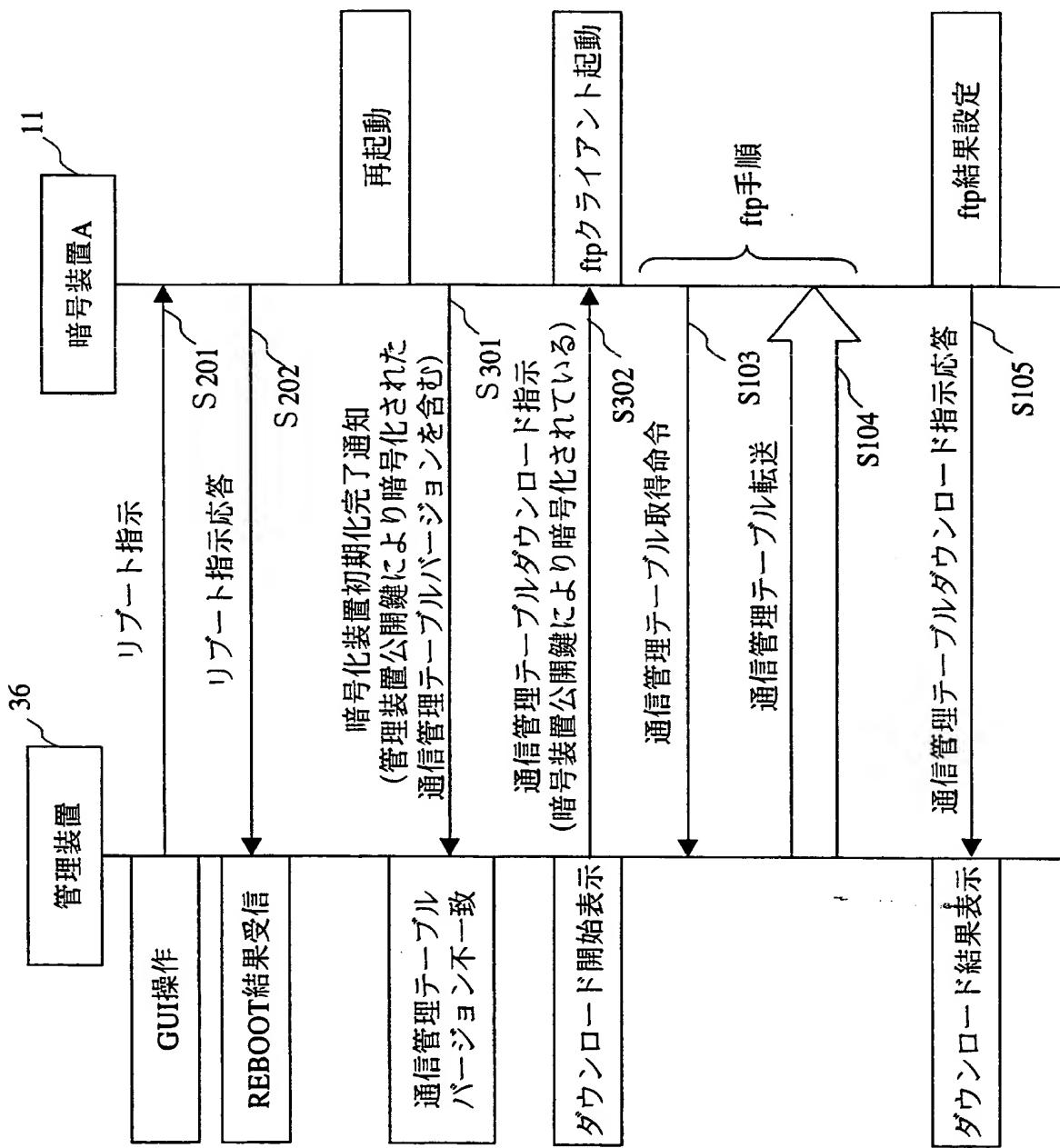
4



5/15

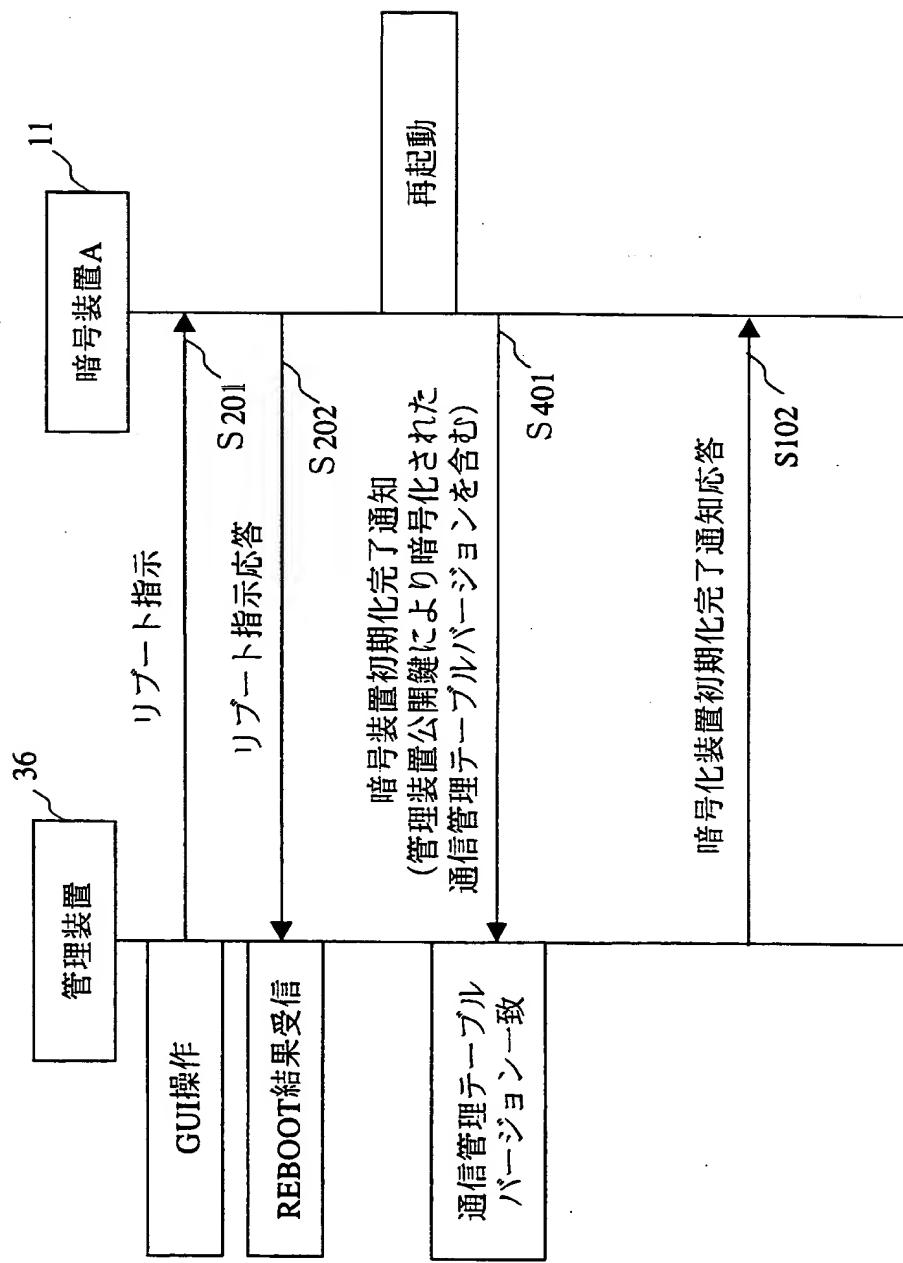
凶

5



6/15

凶 6



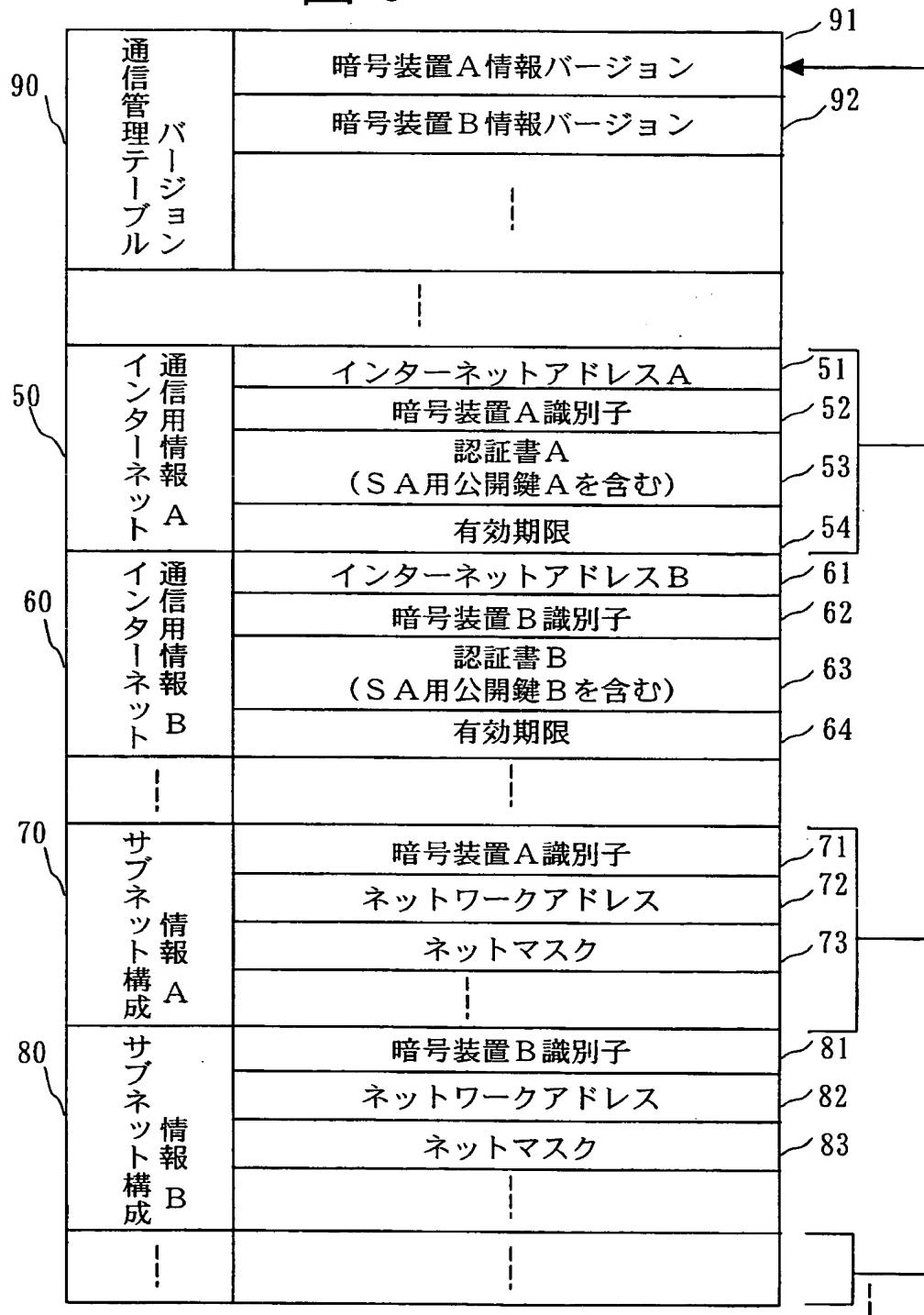
7/15

図 7

| 通信管理テーブルバージョン | |
|--------------------|----------------------------|
| 通信用情報 インターネット A | インターネットアドレス A 52 |
| | 暗号装置 A 識別子 53 |
| | 認証書 A 54 (SA用公開鍵 A を含む) |
| | 有効期限 61 |
| 通信用情報 インターネット B | インターネットアドレス B 62 |
| | 暗号装置 B 識別子 63 |
| | 認証書 B 64 (SA用公開鍵 B を含む) |
| | 有効期限 64 |
| サブネット構成情報 A | 暗号装置 A 識別子 72 |
| | ネットワークアドレス 73 |
| | ネットマスク 81 |
| | |
| サブネット構成情報 B | 暗号装置 B 識別子 82 |
| | ネットワークアドレス 83 |
| | ネットマスク |
| | |

8/15

図 8



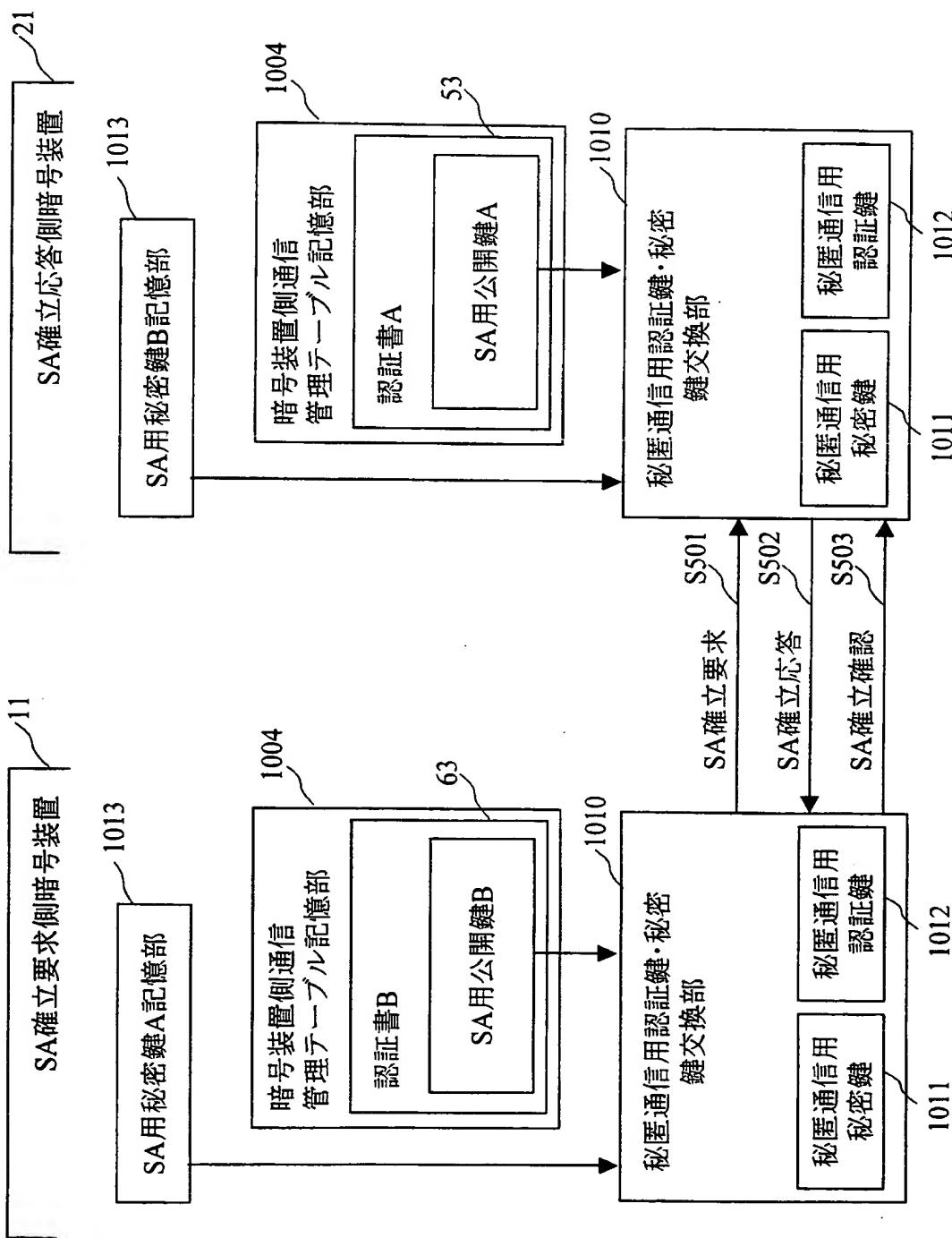
9/15

図 9

| | | |
|------------|----------------------------|----|
| 通信管理バージョン | 暗号装置Aインターネット 通信用情報バージョン | 93 |
| | 暗号装置Aサブネット 構成情報バージョン | 94 |
| | 暗号装置Bインターネット 通信用情報バージョン | 95 |
| | 暗号装置Bサブネット 構成情報バージョン | 96 |
| | ⋮ | ⋮ |
| 通信用情報ネットA | インターネットアドレスA | 51 |
| | 暗号装置A識別子 | 52 |
| | 認証書A (SA用公開鍵Aを含む) | 53 |
| | 有効期限 | 54 |
| 通信用情報ネットB | インターネットアドレスB | 61 |
| | 暗号装置B識別子 | 62 |
| | 認証書B (SA用公開鍵Bを含む) | 63 |
| | 有効期限 | 64 |
| サブネット構成A情報 | ⋮ | ⋮ |
| | 暗号装置A識別子 | 71 |
| | ネットワークアドレス | 72 |
| | ネットマスク | 73 |
| サブネット構成B情報 | ⋮ | ⋮ |
| | 暗号装置B識別子 | 81 |
| | ネットワークアドレス | 82 |
| | ネットマスク | 83 |
| ⋮ | ⋮ | ⋮ |

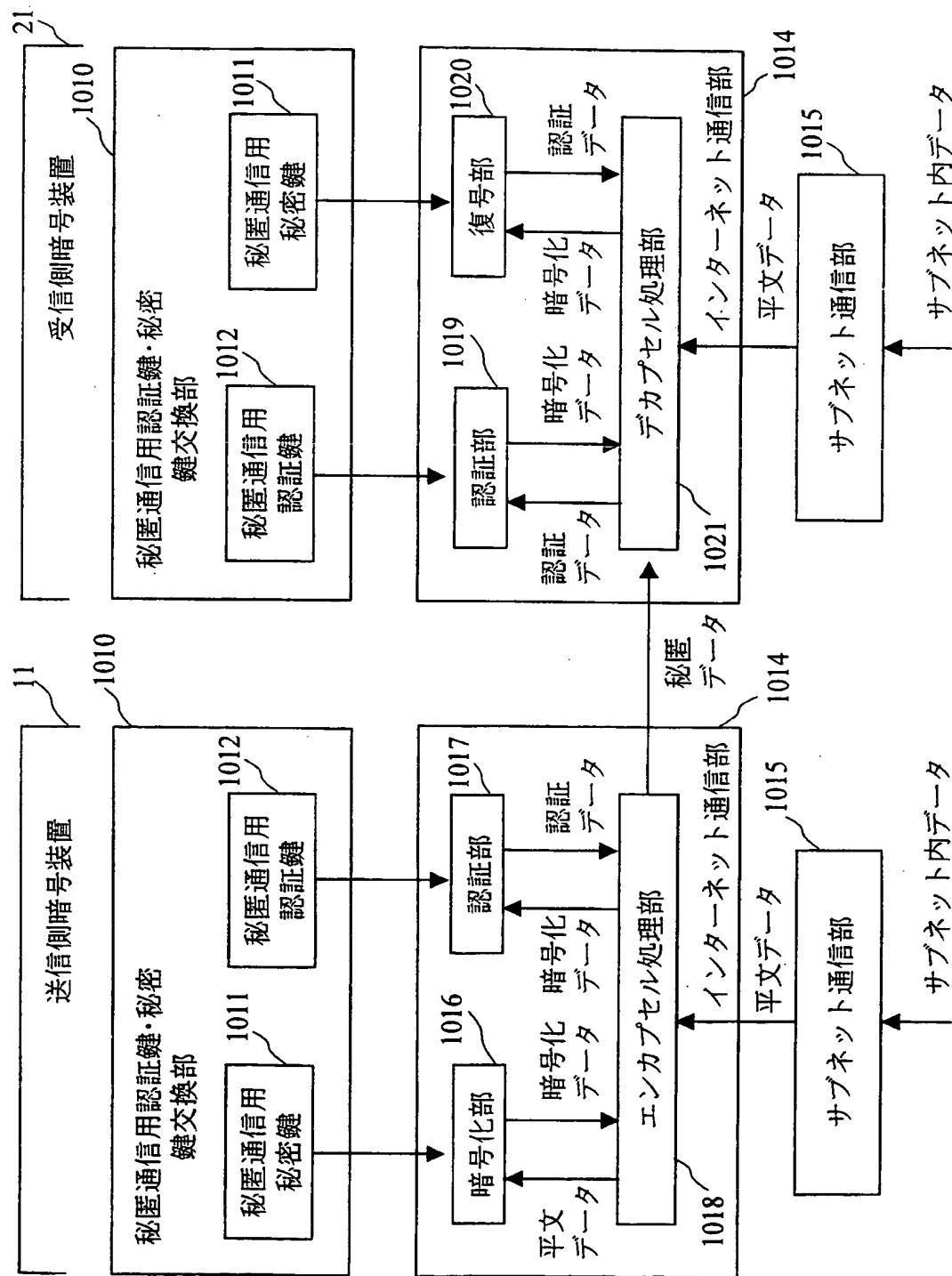
10/15

図 10

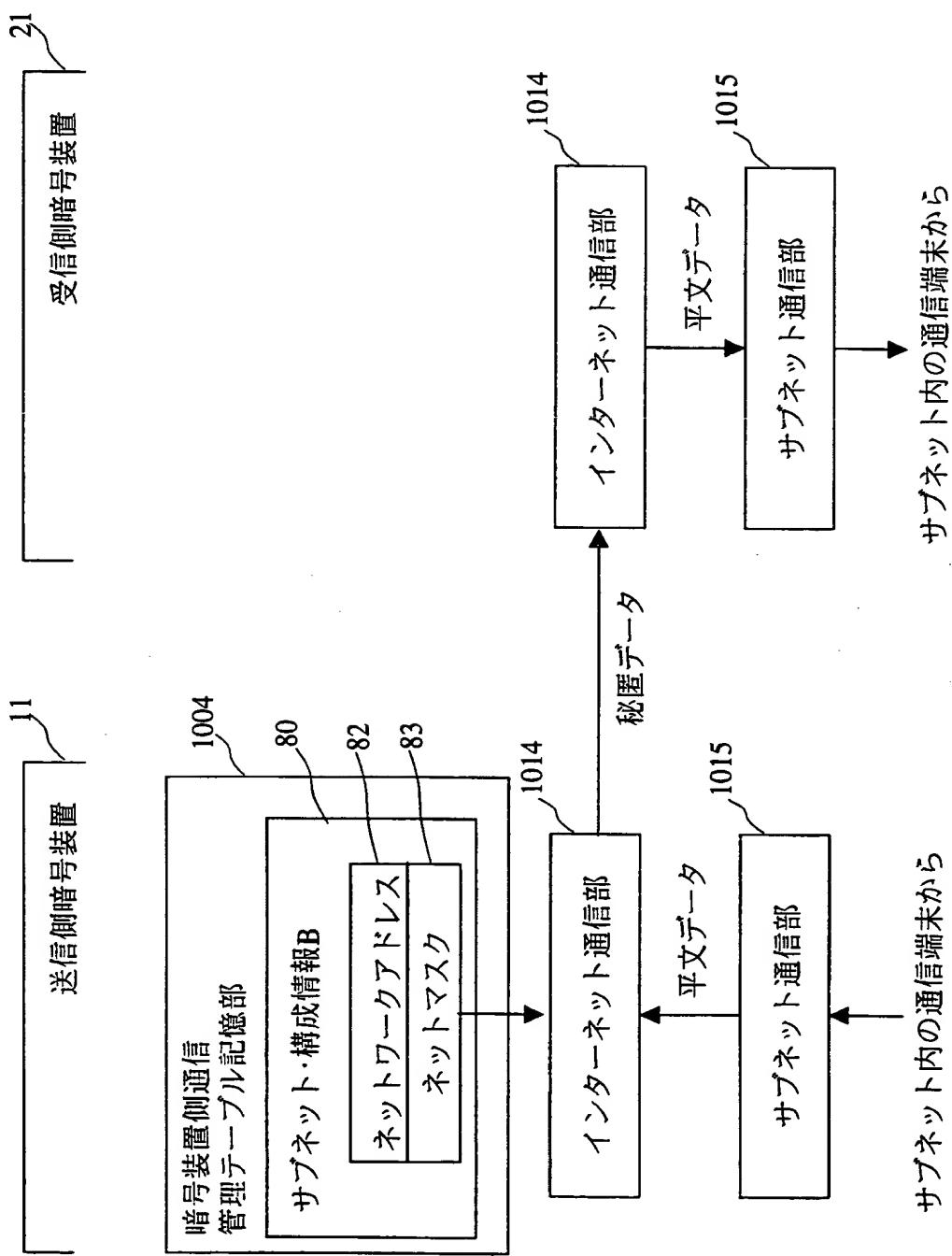


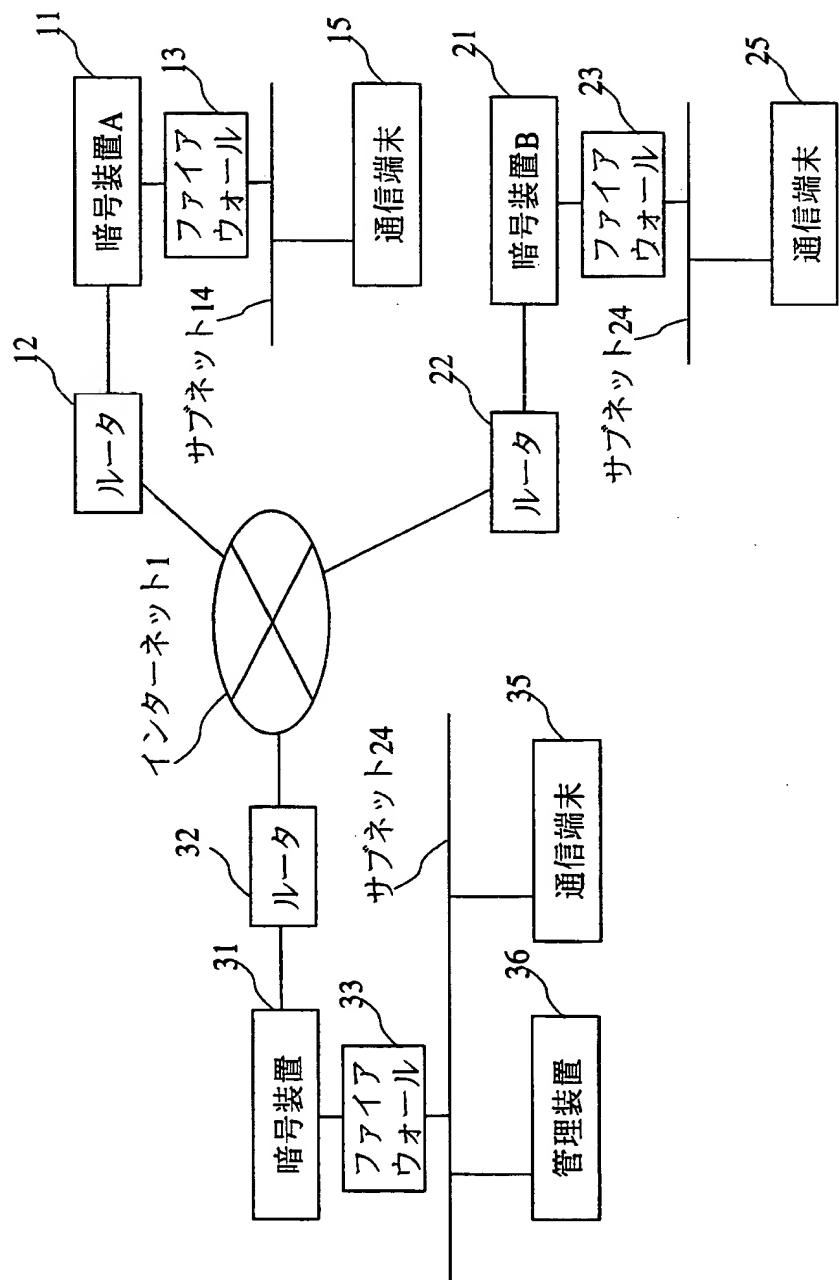
11/15

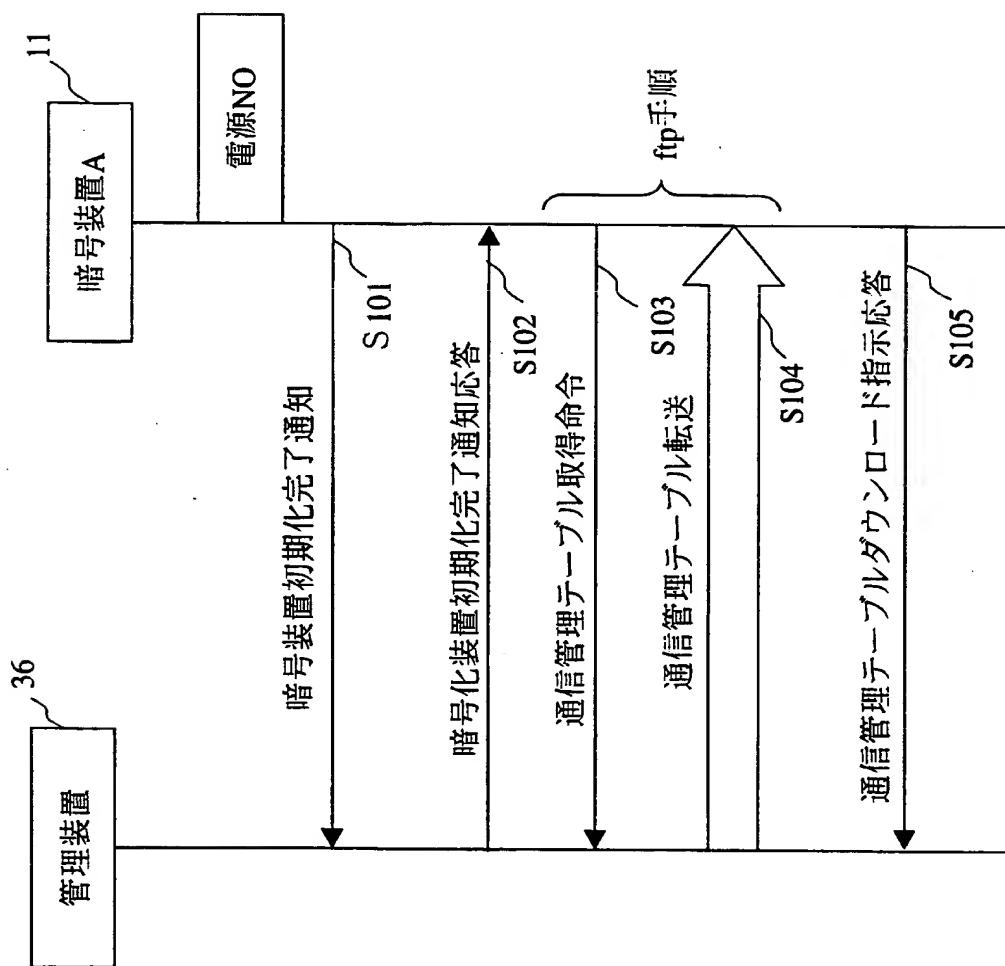
11



12/15
四 12

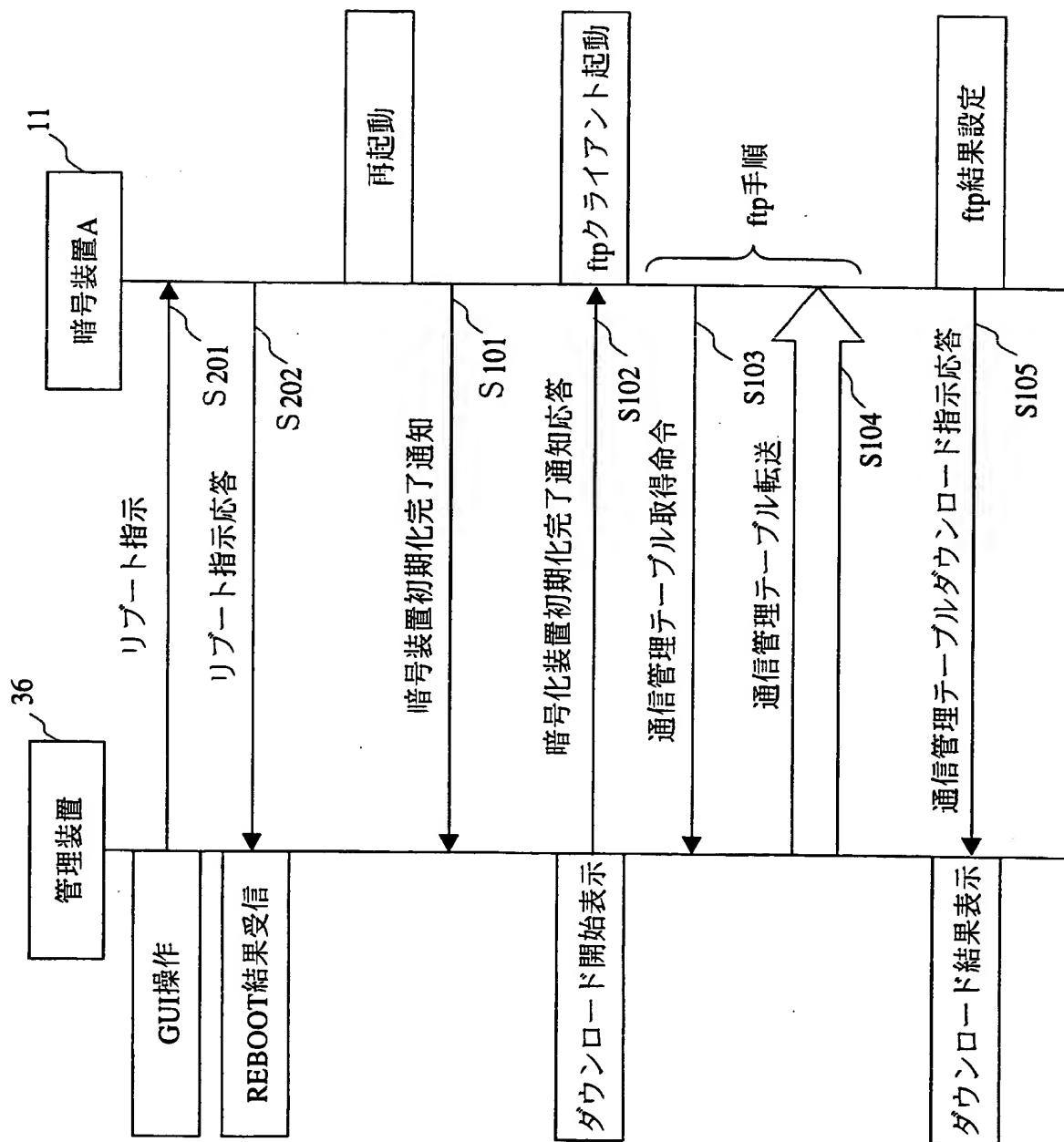


13/15
図 13

14/15
図 14

15/15

四 15



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00474

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L 9/08, H04L 29/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G09C 1/00- 5/00, H04K 1/00-3/00, H04L 9/00, H04L 29/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y | Paul Albits and Criket Liu, Supervisors of translation: Hiroaki TAKADA, Ikuo KOJIMA; Translator: Mitsumasa KODATE, "DNS & BIND the 3 rd ed.", the 2 nd ed., Orairii Japan, (03 June, 1999), pp. vii-ix, 100-102 | 1-12 |
| Y | RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions," (Jan 1997) | 1-12 |
| A | RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," (Nov 1987) | 1-12 |

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| | |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Date of the actual completion of the international search 13 April, 2000 (13.04.00) | Date of mailing of the international search report 25 April, 2000 (25.04.00) |
| Name and mailing address of the ISA/ Japanese Patent Office | Authorized officer |
| Facsimile No. | Telephone No. |

国際調査報告

国際出願番号 PCT/JP00/00474

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl'

H04L 9/08

H04L 29/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl'

G09C 1/00 - 5/00

H04L 9/00

H04K 1/00 - 3/00

H04L 29/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

INSPEC (DIALOG)

C. 関連すると認められる文献

| 引用文献の カテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する 請求の範囲の番号 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|------------------|
| Y | Paul Albits and Criket Liu, 高田広章, 小島育夫監訳, 小館光正訳, 「DNS & BIND 第3版」第2版, オライリー・ジャパン, (1999年6月3日), pp. vii-ix, 100-102 | 1-12 |
| Y | RFC (Request for Comments) 2065, D. Eastlake, 3rd and C. Kaufman, "Domain Name System Security Extensions," (Jan 1997) | 1-12 |
| A | RFC (Request for Comments) 1035, P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," (Nov 1987) | 1-12 |

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

13.04.00

国際調査報告の発送日

25.04.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

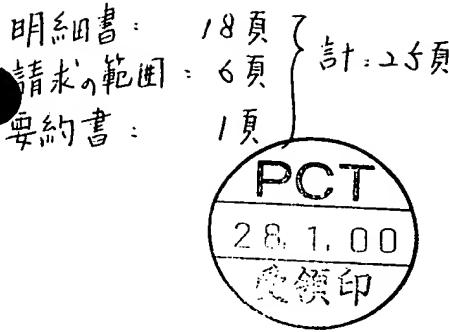
特許庁審査官 (権限のある職員)

丸山 高政

5W 9570



電話番号 03-3581-1101 内線 9570



明細書

通信管理テーブル転送システム及び管理装置及び暗号装置及び通信管理テーブル転送方法

5

技術分野

本発明は、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上に関する。

背景技術

近年、仮想私設網（VPN：Virtual Private Network）を用いるシステムが普及している。仮想私設網は、データの暗号化やユーザ認証などのセキュリティ技術を用いてインターネット等のパブリックネットワークを仮想的（Virtual）に専用線（Private Network）のように利用するネットワークのことである。仮想私設網によって、複数の組織における内部ネットワーク間を専用線を用いるかのごとく接続することができる。

図13は、仮想私設網を用いるシステムの例を示す図である。1は、インターネット、11、21、31は、暗号装置、12、22、32は、ルータ、13、23、33は、ファイアウォール、14、24、34は、サブネット（内部ネットワーク）、15、25、35は、通信端末、36は、管理装置である。それぞれ、図のように接続されている。

インターネットを介したデータ転送を行なう場合、外部からの攻撃に対する防御手段としてIP securityに準拠するシステムが用

いられる。IP securityは、インターネット通信規約標準化機関IETF (Internet Engineering Task Force) で定められたIPパケットレベルにおけるセキュリティ確保方式のことである。

5 IP securityでは、各内部ネットワーク上の暗号装置間で、SA (Security Association) という関係を確立した上で、データの転送を行なう。これにより、秘匿通信が可能となる。しかし、SAを確立する為には、その前提として公開鍵を暗号装置間で共有化しておく必要がある。

10 また、内部ネットワーク上の通信端末に対してデータを転送する場合には、各内部ネットワークの構成情報を知っておく必要もある。

そのため、上記の公開鍵や内部ネットワークの構成情報を含む通信管理テーブルを生成し、SAの確立の前にこの通信管理テーブルを暗号装置間で交換する。このような通信管理テーブルを作成し、更新し、配信するためには管理装置36が設置される。

従来、暗号装置から通信管理テーブルを求められた管理装置36は、無条件に通信管理テーブルを暗号装置へ配信していた。

20 図14は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。暗号装置A11の電源がいれられると、暗号装置A11は、暗号装置初期化通知 (S101) を送信する。管理装置36は、暗号装置初期化通知 (S101) を受信すると、暗号装置初期化通知応答 (S102) を送信する。暗号装置A11は、暗号装置初期化通知応答 (S102) を受信すると無条件に通信管理テーブル取得命令 (S103) を発行し、通信管理テーブル転送 (S104) が行なわれる。

また、図15は、従来例におけるリブートされたときの通信管理テー

ブルの転送の手順を示す図である。管理装置 3 6 が、リブート指示 (S 2 0 1) を送信し、暗号装置 A 1 1 が、リブート指示応答 (S 2 0 2) を送信した後、再起動する。これ以降、図 1 4 と同様に動作する。

5 上述のシステムにおいては、通信管理テーブルの転送回数が多く、データ転送の性能を劣化させていた。

また、通信管理テーブルを盗用される機会を増加させ、セキュリティ上の問題があった。つまり、公開鍵や内部ネットワークの構成情報を盗まれ、暗号装置間のデータ転送の秘匿が守られないおそれがあった。

10 本発明は、上記した従来技術の欠点を除くためになされたものであって、通信管理テーブルの転送回数を減らし、データ転送の性能を向上させ、通信管理テーブルを盗用される機会を減らし、セキュリティを向上させることを目的とする。

発明の開示

15 この発明に係る通信管理テーブル転送システムは、インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、

20 上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

25 上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、

上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信
5 管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージ
ョン記憶部と、

上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信
する通信管理テーブルバージョン受信部と、

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理裝
10 置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブ
ルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場
合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送
信部とを備え、

15 上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テ
ーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受
信部により受信された上記管理装置側通信管理テーブルを、上記暗号裝
置側通信管理テーブルとして記憶することを特徴とする。

20 上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判
定部により不一致と判定された場合に、更に、上記管理装置側通信管理
テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理裝
置側通信管理テーブルバージョンを受信し、

25 上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理
テーブル受信部により受信された上記管理装置側通信管理テーブルバ

ジョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする。

この発明に係る管理装置は、インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置で

5 あって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージ

10 ョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

15

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送

20

信部とを備えることを特徴とする。

上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする。

25

上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする。

上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする。

この発明に係る暗号装置は、インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であって、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

10 上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

15 上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする。

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

25 上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶する

ことを特徴とする。

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする。
5

上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする。
10

上記他の暗号装置は、サブネットに接続し、

上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

15 上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴とする。

この発明に係る通信管理テーブル転送方法は、インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、

20 上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信

管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

5 上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、

10 上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、

上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、

15 上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする。

図面の簡単な説明

図1は、本実施例における暗号装置の構成を示す図である。

20 図2は、本実施例における管理装置の構成を示す図である。

図3は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図4は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。

25 図5は、本実施例におけるリポートされたときの通信管理テーブルの転送の手順を示す図である。

図 6 は、本実施例におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。

図 7 は、本実施例における通信管理テーブルの構成を示す図である。

図 8 は、本実施例における通信管理テーブルの構成を示す図である。

5 図 9 は、本実施例における通信管理テーブルの構成を示す図である。

図 10 は、S A 確立の際のデータフローを示す図である。

図 11 は、秘匿通信の際のデータフローを示す図である。

図 12 は、サブネット構成情報の使用例を示す図である。

図 13 は、仮想私設網を用いるシステムの例を示す図である。

10 図 14 は、従来例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。

図 15 は、従来例におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。

15 発明を実施するための最良の形態

実施の形態 1.

以下、本発明を図面に示す実施例に基づいて説明する。

図 1 は、本実施例における暗号装置の構成を示す図である。1001 は、電源制御部、1002 は、リブート制御部、1003 は、初期化部、1004 は、暗号装置側通信管理テーブル記憶部、1005 は、暗号装置側通信管理テーブルバージョン記憶部、1006 は、通信管理テーブルバージョン暗号化部、1007 は、初期化完了通知部、1008 は、通信管理テーブルダウンロード制御部、1009 は、通信管理テーブル受信部である。

25 図 2 は、本実施例における管理装置の構成を示す図である。2001 は、リブート指示部、2002 は、初期化完了受信部、2003 は、通

信管理テーブルバージョン復号部、2004は、管理装置側通信管理テーブル記憶部、2005は、管理装置側通信管理テーブルバージョン記憶部、2006は、通信管理テーブルバージョン判定部、2007は、通信管理テーブルダウンロード指示部、2008は、通信管理テーブル送信部である。

5 図3は、本実施例における電源を入れたときの通信管理テーブルの転送の手順を示す図である。以下、この手順について、図1及び図2の構成に基づいて説明する。

暗号装置A11側では、電源が入れられると、電源制御部1001が
10 初期化部1003に初期化を指示する。初期化部1003は、初期化を完了すると初期化完了通知部1007に初期化の完了を知らせる。初期化完了通知部1007は、管理装置36の初期化完了受信部2002に暗号装置初期化完了通知(S301)を送信する。このとき管理装置3
15 6の公開鍵により暗号化した通信管理テーブルバージョンが、暗号装置初期化完了通知(S301)に含まれている。

通信管理テーブルバージョンは、暗号装置側通信管理テーブルバージョン記憶部1005に記憶されている。暗号装置側通信管理テーブルバージョン記憶部1005の通信管理テーブルバージョンは、暗号装置側通信管理テーブル記憶部1004の通信管理テーブルと対応付けられている。この例では、暗号装置側通信管理テーブルバージョン記憶部10
20 05は、暗号装置側通信管理テーブル記憶部1004に含まれるが、別個に設けても構わない。

通信管理テーブルバージョン暗号化部1006は、暗号装置側通信管理テーブルバージョン記憶部1005から通信管理テーブルバージョンを読み、これを暗号化し、暗号化された通信管理テーブルバージョンを初期化完了通知部1007に送るように構成されている。

管理装置 3 6 側では、初期化完了受信部 2 0 0 2 が、暗号装置初期化完了通知 (S 3 0 1) を受信し、通信管理テーブルバージョン復号部 2 0 0 3 が、暗号化されている通信管理テーブルバージョンを復号する。一方、通信管理テーブルバージョン判定部 2 0 0 6 は、管理装置側通信管理テーブルバージョン記憶部 2 0 0 5 から管理装置 3 6 側で記憶する通信管理テーブルバージョンを読む。そして、通信管理テーブルバージョン判定部 2 0 0 6 は、これらの通信管理テーブルバージョンを比較する。尚、この実施例では、管理装置側通信管理テーブルバージョン記憶部 2 0 0 5 は、管理装置側通信管理テーブル記憶部 2 0 0 4 に含められているが、通信管理テーブルと通信管理テーブルバージョンが対応付けられていれば、別個に設けても構わない。

比較の結果、2つの通信管理テーブルバージョンが不一致の場合には、通信管理テーブルバージョン判定部 2 0 0 6 は、通信管理テーブルダウンロード指示部 2 0 0 7 に不一致を知らせる。

15 通信管理テーブルダウンロード指示部 2 0 0 7 は、不一致の知らせを受けると、暗号装置 A 1 1 の通信管理テーブルダウンロード制御部 1 0 0 8 に通信管理テーブルダウンロード指示 (S 3 0 2) を送信する。

暗号装置 A 1 1 側では、通信管理テーブルダウンロード制御部 1 0 0 8 が、通信管理テーブルダウンロード指示 (S 3 0 2) を受信するとファイル転送の手順に従って通信管理テーブルを受信する為に、通信管理テーブル受信部 1 0 0 9 に通信管理テーブル取得の指示を送る。

通信管理テーブル受信部 1 0 0 9 は、その指示を受けると、管理装置 3 6 の通信管理テーブル送信部 2 0 0 8 に通信管理テーブル取得命令 (S 1 0 3) を送る。

25 管理装置 3 6 側では、通信管理テーブル取得命令 (S 1 0 3) を受けた通信管理テーブル送信部 2 0 0 8 は、管理装置側通信管理テーブル記

憶部 2004 から通信管理テーブルを読み、その通信管理テーブルを暗号装置 A11 の通信管理テーブル受信部 1009 にファイル転送する (S104)。

暗号装置 A11 側では、通信管理テーブル受信部 1009 が通信管理テーブルを受信し終えると、通信管理テーブルダウンロード制御部 1008 に通信管理テーブル取得の完了を知らせ、通信管理テーブルダウンロード制御部 1008 は通信管理テーブルダウンロード指示応答 (S105) を管理装置 36 の通信管理テーブルダウンロード指示部 2007 に送信する。また、通信管理テーブル受信部 1009 は、受信した通信管理テーブルを暗号装置側通信管理テーブル記憶部 1004 に記憶する。
。

この例では、ファイル転送のときに通信管理テーブルに通信管理テーブルバージョンを含めて転送し、暗号装置側通信管理テーブル記憶部 1004 は通信管理テーブルバージョンを含む通信管理テーブル記憶している。しかし、通信管理テーブルバージョンを、通信管理テーブルに含めない構成にすることもできる。つまり、通信管理テーブルバージョンを含まない通信管理テーブルと、通信管理テーブルバージョンを別個にファイル転送することも可能である。

このようにして、通信管理テーブルバージョンが一致しない場合は、通信管理テーブルが管理装置 36 から暗号装置 A11 へ転送される。また、通信管理テーブルバージョンも転送される。

図 4 は、本実施例における電源を入れたときの通信管理テーブルの転送を省略する手順を示す図である。以下、この手順について、図 1 及び図 2 の構成に基づいて説明する。

通信管理テーブルバージョン判定部 2006 が、通信管理テーブルバージョンを比較するまでの手順は、上述の手順と同様である。

比較の結果、通信管理テーブルバージョンが一致した場合には、通信管理テーブルバージョン判定部2006は、一致を初期化完了受信部2002に知らせる。

初期化完了受信部2002は、暗号装置初期化完了通知応答（S105）を初期化完了通知部1007に送信する。初期化完了通知部1007が、暗号装置初期化完了通知応答（S102）を受け取ると動作を終了する。つまり、通信管理テーブルバージョンが一致する場合は、通信管理テーブルの転送は行なわれない。

暗号装置A11が通信管理テーブルバージョンを送信し、管理装置310が通信管理テーブルバージョンを判定するタイミングは、初期化の時に限られない。システムで自由に設定することができる。例えば、リブートのタイミングや、定期的なタイミングであっても構わない。

図5は、本実施におけるリブートされたときの通信管理テーブルの転送の手順を示す図である。また、図6は、本実施におけるリブートされたときの通信管理テーブルの転送を省略する手順を示す図である。リブート指示（S201）とリブート指示応答（S202）に基づく再起動から始まる点を除き、図3及び図4の手順と同様である。

次に、通信管理テーブルの構成について説明する。図7、図8及び図9は本実施例における通信管理テーブルの構成を示す図である。

通信管理テーブルには、通信管理テーブルバージョン90のほか、インターネット通信用情報A50、インターネット通信用情報B60等のインターネット通信用情報と、サブネット構成情報A70、サブネット構成情報B80等のサブネット構成情報が含まれる。

インターネット通信用情報A50は、暗号装置A11がインターネット1を介して、他の暗号装置と通信する場合に必要になる情報である。インターネット通信用情報B60も同様に、暗号装置B21がインターネット

ネット 1 を介して、他の暗号装置と通信する場合に必要になる情報である。

5 1、6 1 は、インターネットアドレス、5 2、6 2 は、暗号装置の識別子、5 3、6 3 は、認証書、5 4、6 4 は有効期限である。認証書
5 には、S A 用公開鍵が含まれている。

サブネット構成情報 A 7 0 は、サブネット 1 4 の構成に関する情報である。この図では、1 レコードのみ示しているが、サブネット 1 4 の構成に含まれる通信端末が多い場合には、更にレコードが付加されている。サブネット構成情報 B 8 0 も同様である。

10 7 1、8 1 は、暗号装置の識別子、7 2、8 2 は、ネットワークアドレス、7 3、8 3 は、ネットマスクである。

図 7 の例では、通信管理テーブルバージョン 9 0 は、バージョンは一つであり、通信管理テーブル全体の更新状況に対応している。

15 図 8 の例では、通信管理テーブルバージョン 9 0 は、暗号装置 A 情報バージョン 9 1、暗号装置 B 情報バージョン 9 2 等複数のバージョンから構成されている。暗号装置 A 情報バージョン 9 1 は、インターネット通信用情報 A 5 0 とサブネット構成情報 A 7 0 等（サブネット構成情報 A 7 0 の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

20 図 9 の例では、更に細分化し、通信管理テーブルバージョン 9 0 は、暗号装置 A インターネット通信用情報バージョン 9 3、暗号装置 A サブネット構成情報バージョン 9 4、暗号装置 B インターネット通信用情報バージョン 9 5、暗号装置 B サブネット構成情報バージョン 9 6 等のバージョンから構成されている。暗号装置 A インターネット通信用情報バージョン 9 3 は、インターネット通信用情報 A 5 0 の更新状況に対応している。また、暗号装置 A サブネット構成情報バージョン 9 4 は、サブ

ネット構成情報A70等（サブネット構成情報A70の他にサブネット構成情報がある場合にはそれらも含む。）の更新状況に対応している。

図8と図9の場合に、バージョンと各情報との対応をつけるために、各バージョンに対応して装置識別子や情報識別子を記憶する方法も考えられる。

管理装置36は、各暗号装置から、通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部（図示せず）と、管理装置側通信管理テーブルと、管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部（図示せず）を有する。

図7の場合、通信管理テーブル更新情報受信部は、いずれの暗号装置から通信管理テーブル更新情報を受信した場合にも、通信管理テーブルバージョン90を更新する。図8の場合、通信管理テーブル更新情報受信部は、暗号装置A11から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報A50、サブネット構成情報A70のいずれか若しくは両方を更新し、更に暗号装置A情報バージョン91を更新する。図9の場合、通信管理テーブル更新情報受信部は、暗号装置A11から通信管理テーブル更新情報を受信した場合には、インターネット通信用情報A50に関する通信管理テーブル更新情報、サブネット構成情報A70に関する通信管理テーブル更新情報のいずれか若しくは両方かを判断し、その部分を更新し、更にその部分に対応する暗号装置Aインターネット通信用情報バージョン93、暗号装置Aサブネット構成情報バージョン94のいずれか若しくは両方を更新する。

図8や図9のように、通信管理テーブルバージョンを細分化した場合には、通信管理テーブルバージョン判定部2006は、細分化したバージョン毎に比較し、通信管理テーブルのうち不一致のバージョンに関する

る部分のみを通信管理テーブル転送（S 1 0 4）で転送するようにすることも有効である。その場合は、通信管理テーブルダウンロード指示（S 3 0 2）に転送する部分を特定する情報を付加し、通信管理テーブル受信部 1 0 0 9 は、暗号装置側通信管理テーブル記憶部 1 0 0 4 の中の 5 その部分のみを更新し、暗号装置側通信管理テーブルバージョン記憶部 1 0 0 5 の中のその部分のバージョンのみを更新する。

次に、通信管理テーブルに含まれる S A 用公開鍵を用いて S A を確立する動作について説明する。図 1 0 は、 S A 確立の際のデータフローを示す図である。この例では、暗号装置 A 1 1 が S A 確立を要求する側で 10 あり、暗号装置 B 2 1 が S A 確立の要求に応答する側である。それぞれの暗号装置は、自らの S A 用秘密鍵を記憶する S A 用秘密鍵記憶部 1 0 1 3 と、秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を共有化する秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 とを有する。秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、図に示すように、自らの S A 用秘密鍵 15 と、相手側の S A 用公開鍵とを入力できるように構成されている。

暗号装置 A 1 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X a を生成し、署名し、暗号化し、暗号装置 B 2 1 側へ送信する（S 5 0 1）。暗号装置 B 2 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X b を生成し、乱数 X a と組合わせて秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を生成する。更に、X b と X a のハッシュ値を署名し、暗号化し、暗号装置 A 1 1 側へ送信する（S 5 0 2）。暗号装置 A 1 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、乱数 X a と乱数 X b とを組合わせて秘匿通信用秘密鍵 1 0 1 1 と秘匿通信用認証鍵 1 0 1 2 を生成し、受信したハッシュ値を検証する。更に乱数 X b のハッシュ値を暗号装置 B 2 1 側に送信する（S 5 0 3）。暗号装置 B 2 1 の秘匿通信用認証鍵秘密鍵交換部 1 0 1 0 は、受信したハッシュ値を検証す 25

る。以上の手順により、S Aが確立する。これによって、両者は、共通の秘匿通信用秘密鍵1011と秘匿通信用認証鍵1012を取得する。

次に、S A確立の後に行われる秘匿通信の動作について説明する。図11は、秘匿通信の際のデータフローを示す図である。この例では、暗号装置A11がデータを送信する側であり、暗号装置B21がデータを受信する側である。但し、S Aが確立している暗号装置間では、双方向の通信が可能であり、この例に限定されない。

それぞれの暗号装置は、インターネット通信部1014と、サブネット通信部1015とを有する。インターネット通信部1014は、インターネット1を介する通信を制御し、サブネット通信部1015は、サブネットを介する通信を制御する。

送信側のインターネット通信部1014は、暗号化部1016と、認証部1017と、エンカプセル処理部1018が動作する。また、受信側のインターネット通信部1014は、認証部1019と、復号部1020と、デカプセル処理部1021が動作する。この動作において、秘匿通信用秘密鍵1011は、暗号アルゴリズムに使用され、秘匿通信用認証鍵1012は、認証アルゴリズムに使用される。

また、通信管理テーブルに含まれるサブネット構成情報は、他の暗号装置に接続されるサブネットに対して通信を行なう場合に用いられる。

図12に示すように、サブネット構成情報は、インターネット通信部1014で用いられる。

産業上の利用可能性

本発明においては、管理装置と暗号装置の間で、通信管理テーブルのバージョンを管理し、両者間の通信管理テーブルの同一性が確認できた場合には、通信管理テーブルの転送を行なわないように構成したので、

通信管理テーブルの転送回数が削減され、データ通信の性能及び安全性が著しく向上する。

請求の範囲

1. インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムであって、
 - 5 上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、
上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、
10 上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部とを備え、
上記管理装置は、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、
15 上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、
20 上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と、
受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、
25 上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送

信部とを備え、

上記暗号装置は、更に、上記管理装置から上記管理装置側通信管理テーブルを受信する通信管理テーブル受信部を備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする通信管理テーブル転送システム。

2. 上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信し、

上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項1記載の通信管理テーブル転送システム。

3. インターネットを介して互いに接続する複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置であって、

上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、

上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部と、

上記暗号装置から、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルのバージョンである暗号装置側通信管理テーブルバージョンを受信する通信管理テーブルバージョン受信部と

受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する通信管理テーブルバージョン判定部と、

5 上記通信管理テーブルバージョン判定部により不一致と判定された場合に、上記管理装置側通信管理テーブルを送信する通信管理テーブル送信部とを備えることを特徴とする管理装置。

4. 上記通信管理テーブル送信部は、上記通信管理テーブルバージョン判定部により不一致と判定された場合に、更に、上記管理装置側通信管理テーブルバージョンを送信することを特徴とする請求項3記載の管理装置。

5. 上記管理装置は、更に、上記管理装置側通信管理テーブルと、上記管理装置側通信管理テーブルバージョンとを対応付けて更新する管理装置側通信管理テーブル更新部を有することを特徴とする請求項3記載の管理装置。

6. 上記管理装置は、更に、上記管理装置側通信管理テーブルの中で更新する情報である通信管理テーブル更新情報を受信する通信管理テーブル更新情報受信部を有することを特徴とする請求項5記載の管理装置。

20 7. インターネットを介して他の暗号装置と接続し、通信に用いる通信管理テーブルを管理装置によって管理される暗号装置であつて、

上記暗号装置は、上記暗号装置で記憶する上記通信管理テーブルである暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、

上記暗号装置側通信管理テーブルのバージョンである暗号装置側通信

管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部と、

上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する通信管理テーブルバージョン送信部と、

5 上記管理装置から、上記管理装置で記憶する上記通信管理テーブルである管理装置側通信管理テーブルを受信する通信管理テーブル受信部とを備え、

上記暗号装置側通信管理テーブル記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶することを特徴とする暗号装置。

8. 上記通信管理テーブル受信部は、更に、上記管理装置から上記管理装置側通信管理テーブルのバージョンである管理装置側通信管理テーブルバージョンを受信し、

上記暗号装置側通信管理テーブルバージョン記憶部は、上記通信管理テーブル受信部により受信された上記管理装置側通信管理テーブルバージョンを、上記暗号装置側通信管理テーブルバージョンとして記憶することを特徴とする請求項 7 記載の暗号装置。

9. 上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用秘密鍵を、上記暗号装置側通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用秘密鍵交換部を備えることを特徴とする請求項 7 記載の暗号装置。

10. 上記通信管理テーブルは、公開鍵を含み、

上記暗号装置は、更に、上記他の暗号装置と上記インターネットを介して秘匿通信を行なう際に用いる秘匿通信用認証鍵を、上記暗号装置側

通信管理テーブルに含まれる上記公開鍵を用いて上記他の暗号装置と共有化する秘匿鍵通信用認証鍵交換部を備えることを特徴とする請求項 7 記載の暗号装置。

11. 上記他の暗号装置は、サブネットに接続し、
5 上記通信管理テーブルは、上記サブネットの構成についての情報であるサブネット構成情報を含み、

上記暗号装置は、更に、上記暗号装置側通信管理テーブルに含まれる上記サブネット構成情報に基づいて、上記他の暗号装置と上記インターネットを介して通信を行なうインターネット通信部を有することを特徴
10 とする請求項 7 記載の暗号装置。

12. インターネットを介して互いに接続し、それぞれ、暗号装置側通信管理テーブルを記憶する暗号装置側通信管理テーブル記憶部と、暗号装置側通信管理テーブルバージョンを記憶する暗号装置側通信管理テーブルバージョン記憶部とを有する複数の暗号装置と、
15 上記複数の暗号装置が通信に用いる通信管理テーブルを管理し、管理装置側通信管理テーブルを記憶する管理装置側通信管理テーブル記憶部と、管理装置側通信管理テーブルバージョンを記憶する管理装置側通信管理テーブルバージョン記憶部とを有する管理装置とからなる通信管理テーブル転送システムの通信管理テーブル転送方法であって、

20 上記暗号装置が、上記暗号装置側通信管理テーブルバージョンを、上記管理装置へ送信する工程と、

上記管理装置が、上記暗号装置から上記暗号装置側通信管理テーブルバージョンを受信する工程と、

上記管理装置が、受信した上記暗号装置側通信管理テーブルバージョンと、上記管理装置側通信管理テーブルバージョンとの不一致を判定する工程と、
25

上記工程で不一致と判定した場合に、上記管理装置が、上記管理装置側通信管理テーブルを送信する工程と、
上記暗号装置が、上記管理装置から上記管理装置側通信管理テーブルを受信する工程と、
5 上記暗号装置が、受信した上記管理装置側通信管理テーブルを、上記暗号装置側通信管理テーブルとして記憶する工程とを有することを特徴とする通信管理テーブル転送方法。

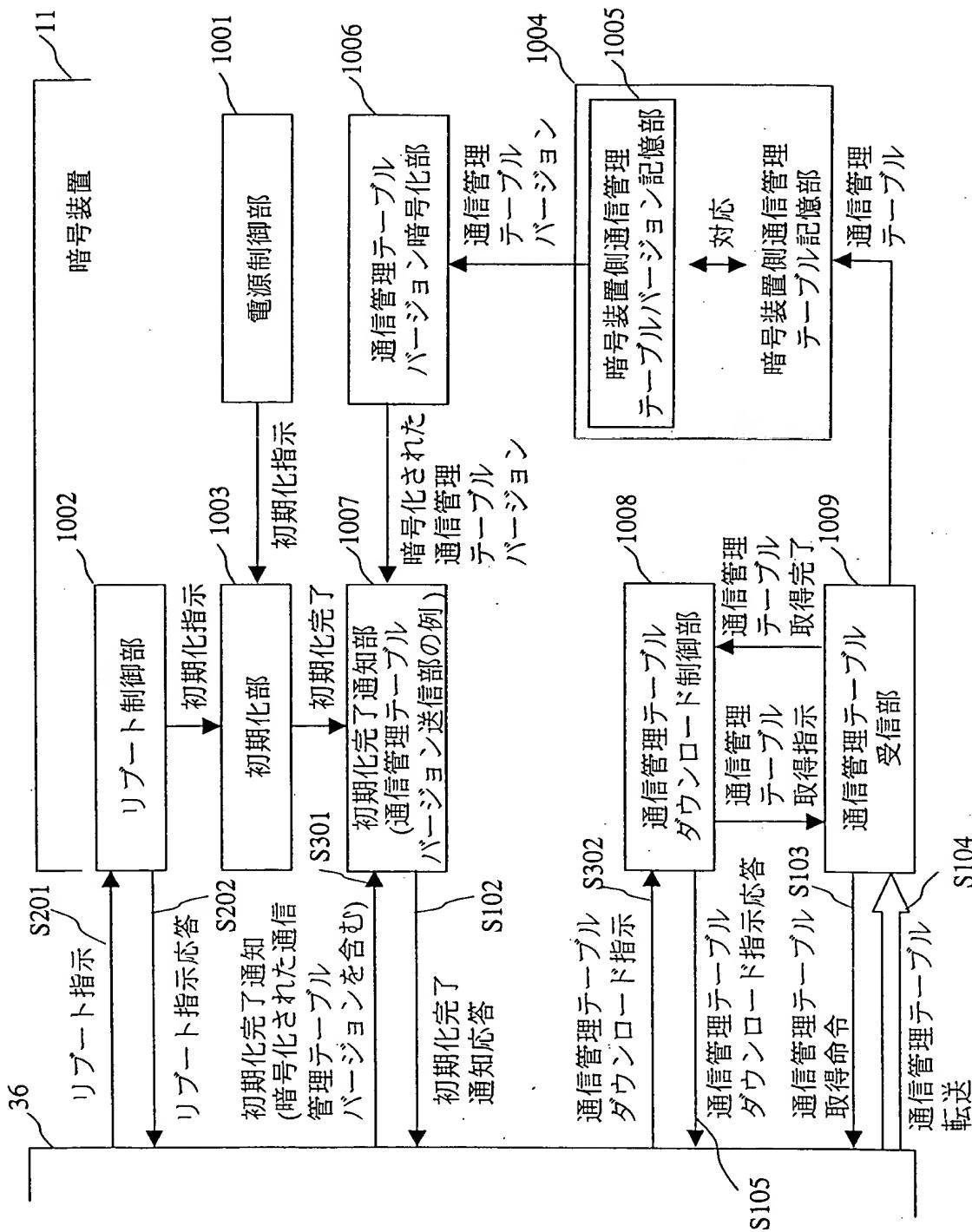
要 約 書

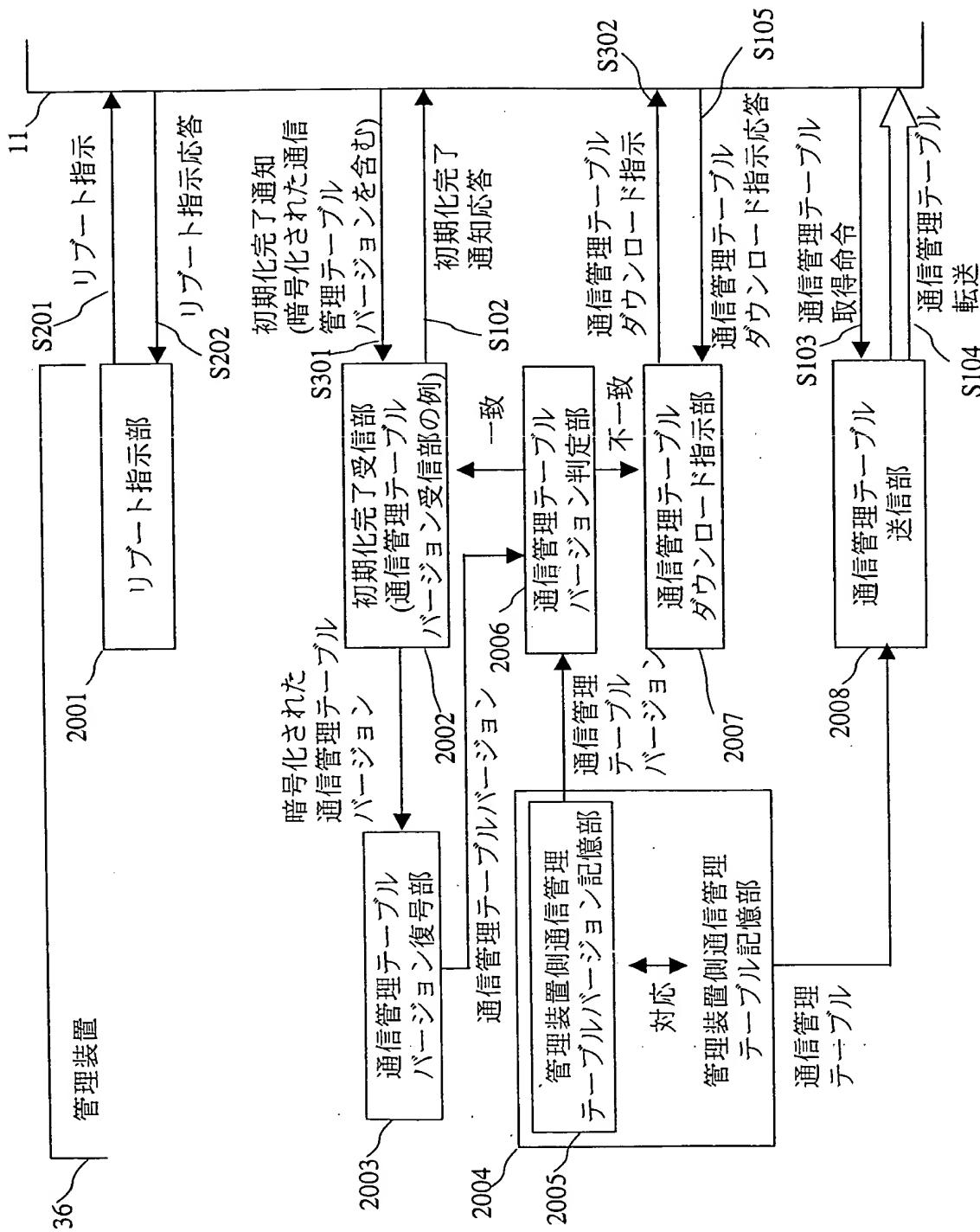
インターネットを介して互いに接続する複数の暗号装置と、上記複数の暗号装置が通信に用いる通信管理テーブルを管理する管理装置とからなる通信管理テーブル転送システムに係り、セキュリティの向上と、性能の向上とを図ることを課題とする。
5

管理装置 36 は、暗号装置 11 から通信管理テーブルバージョンを受信し (S301)、通信管理テーブルバージョン判定部 2006 で、管理装置側通信管理テーブルバージョン記憶部 2005 に記憶している通信管理テーブルバージョンと比較し、不一致の場合にのみ暗号装置 11 10 に対して通信管理テーブルを転送する (S104)。

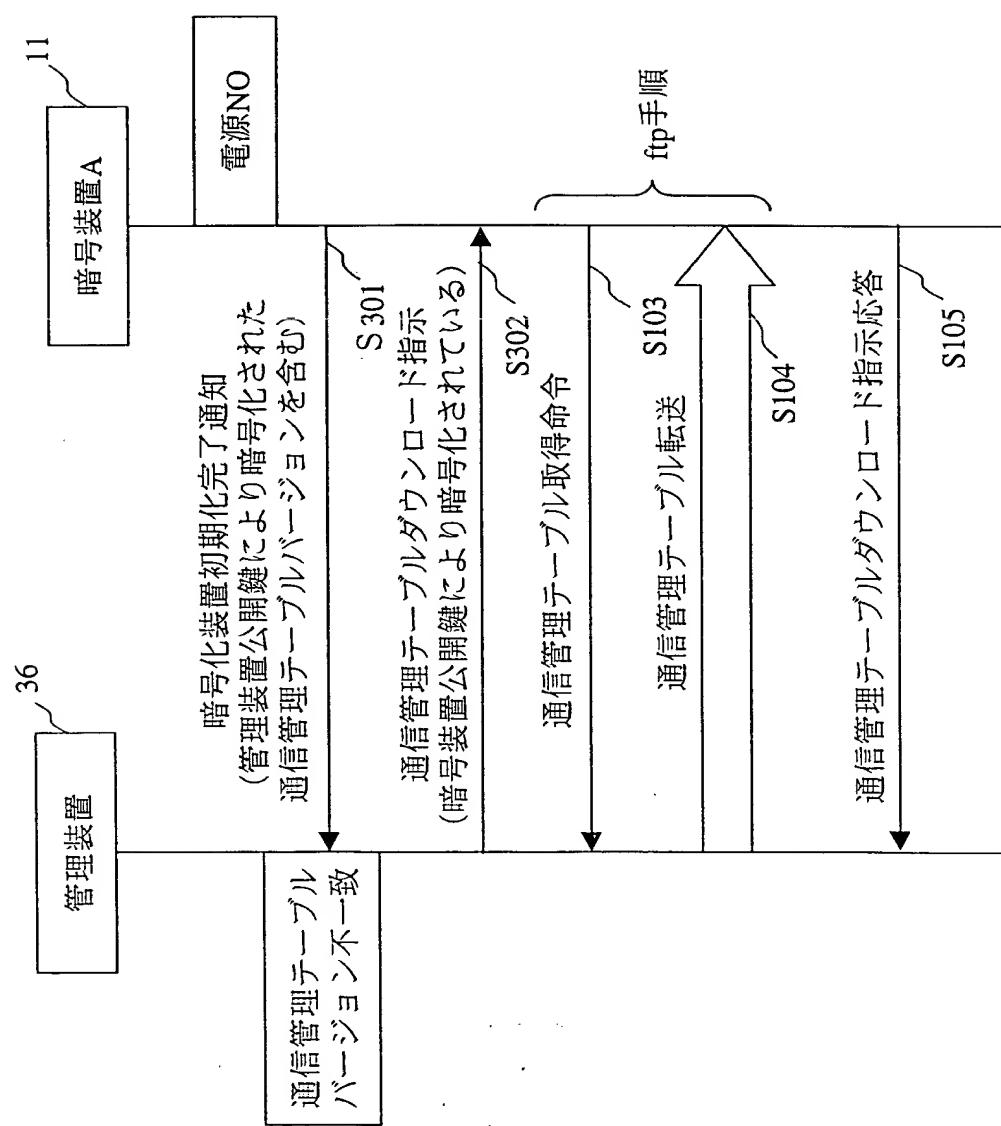
1/15

1

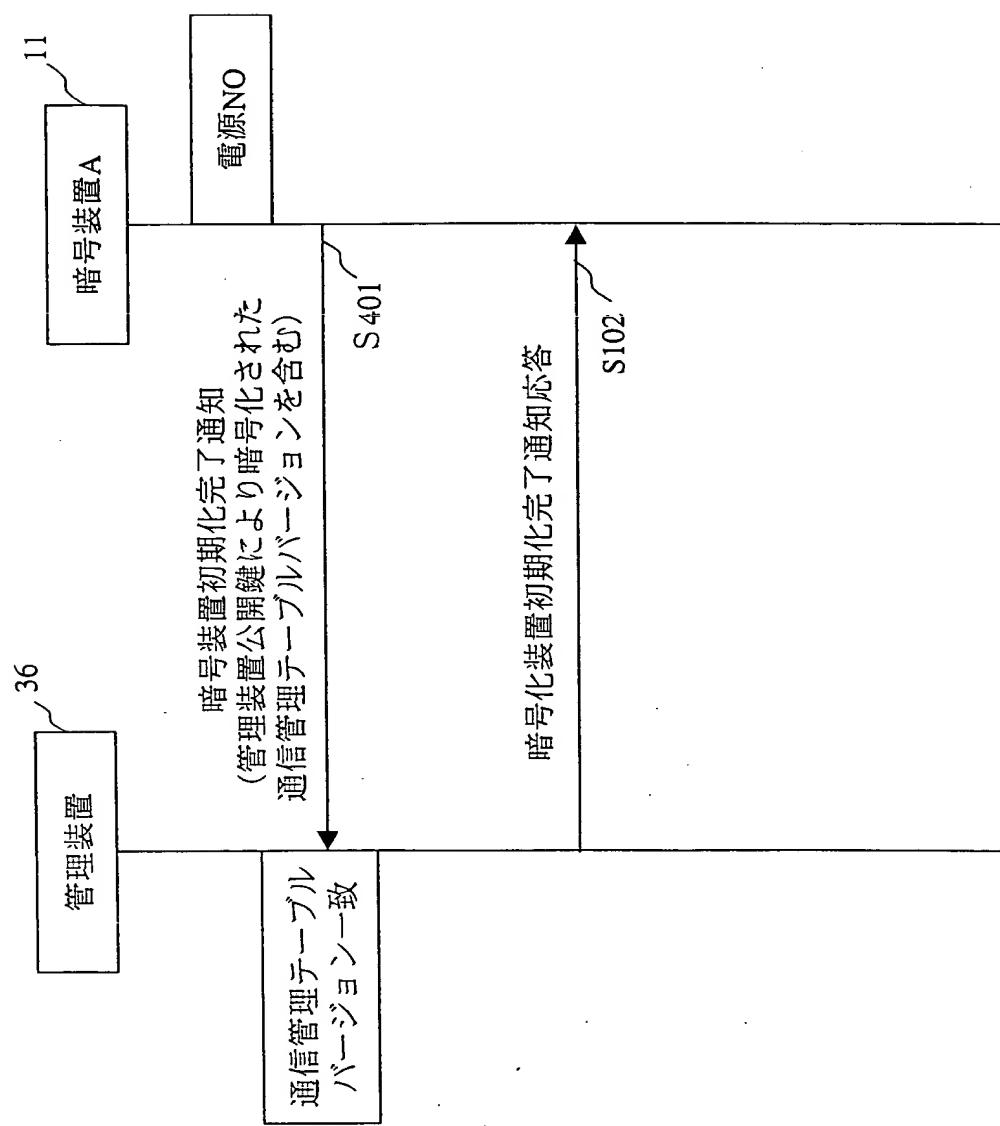




3/15
凶 3



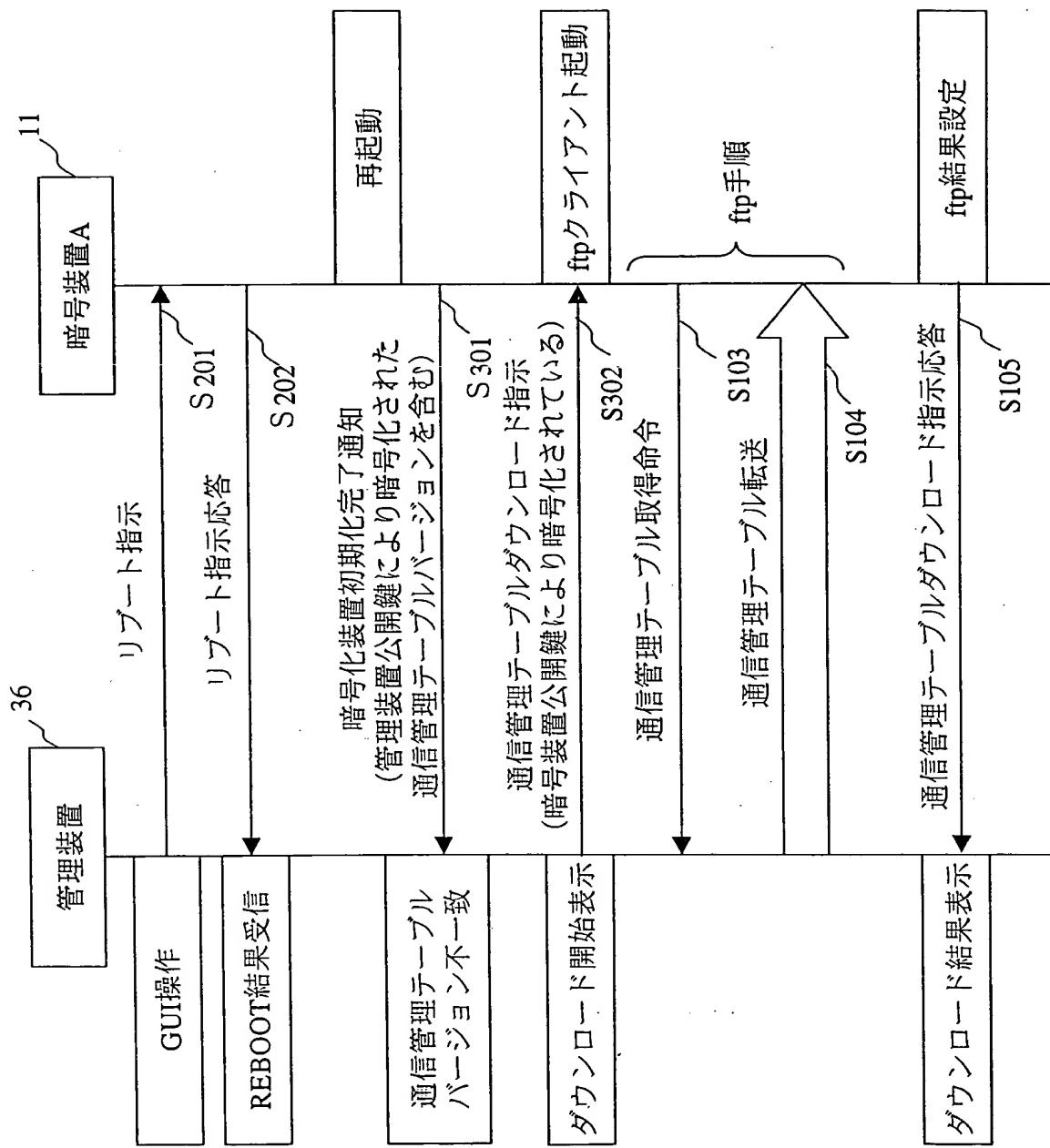
4/15
凶 4



5/15

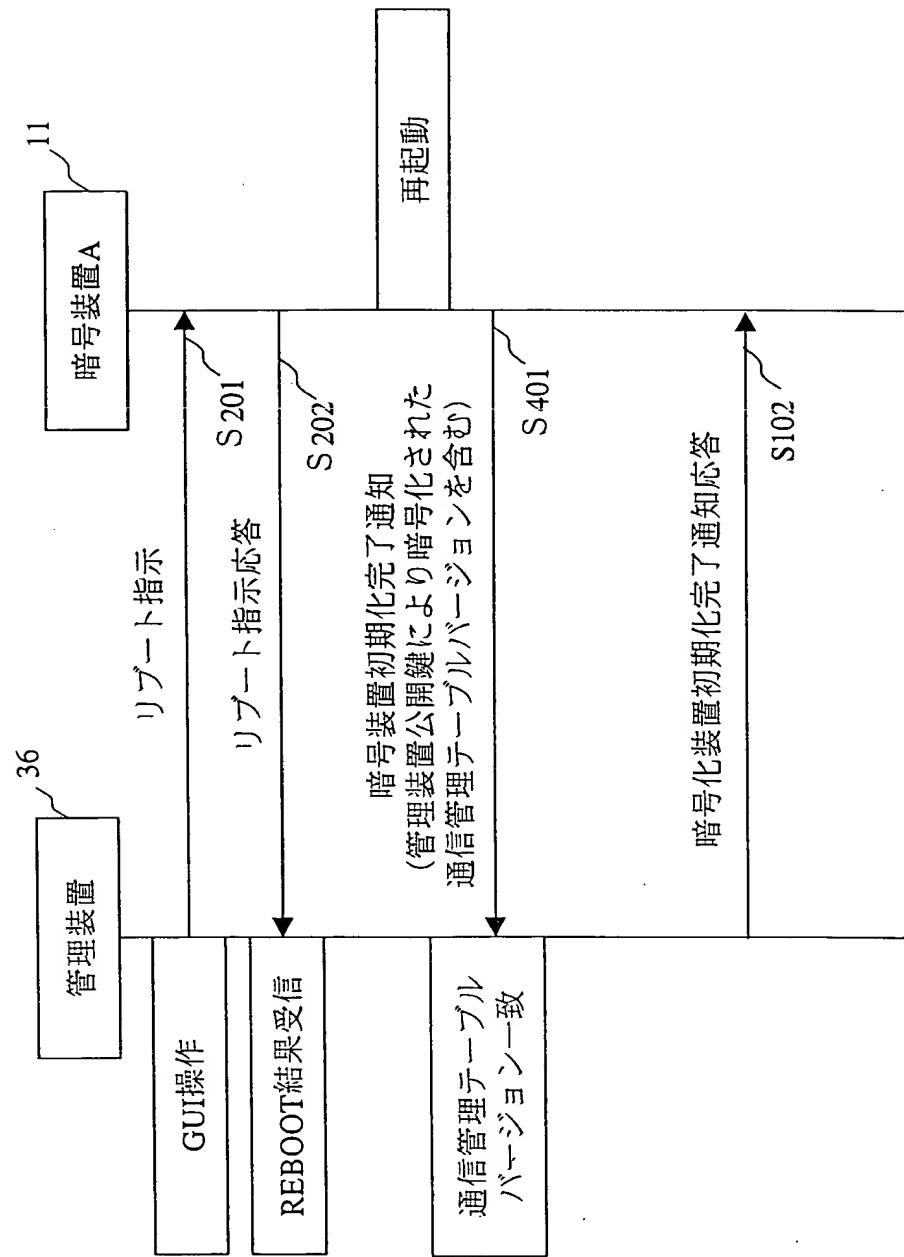
凶

5



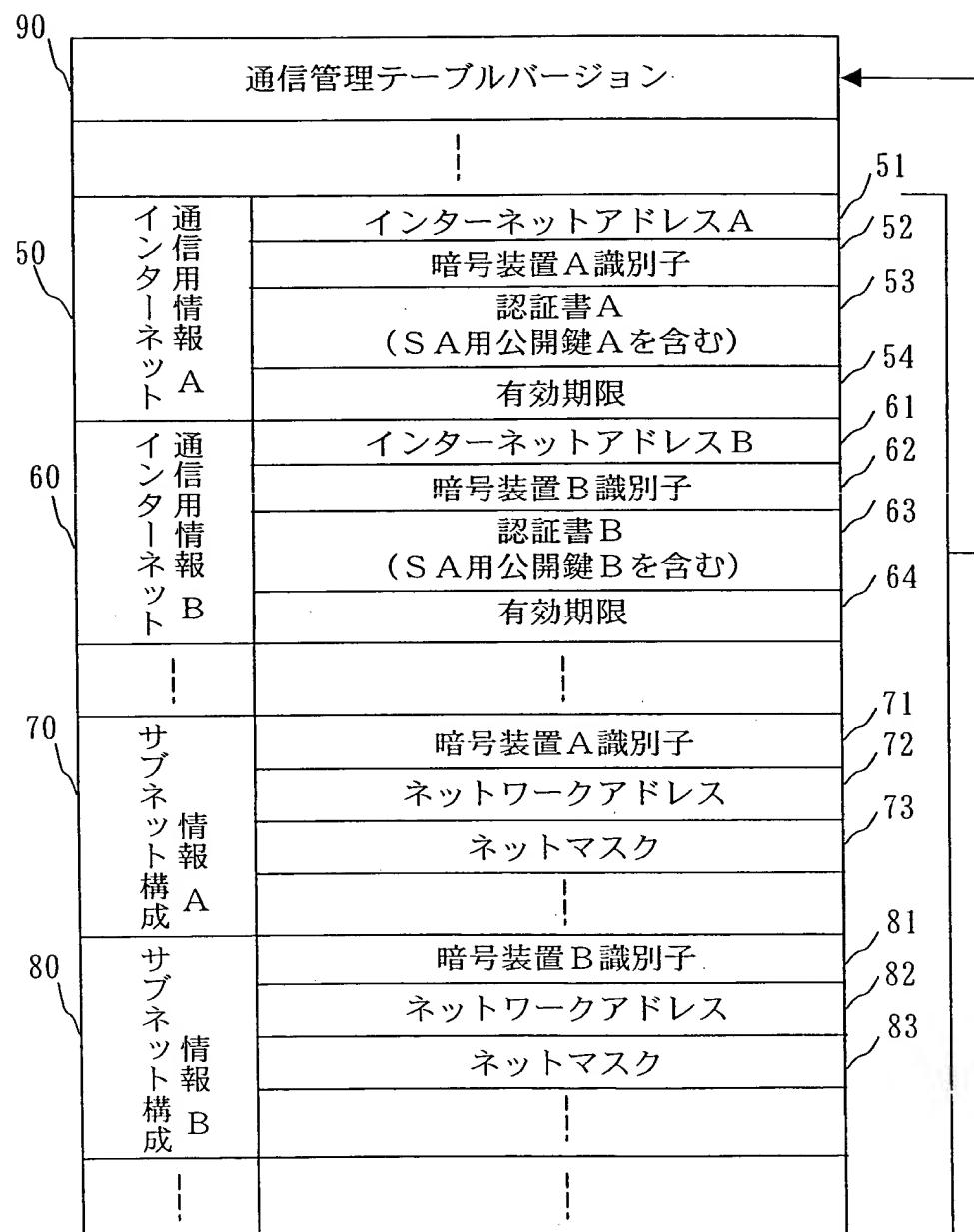
6/15

図 6



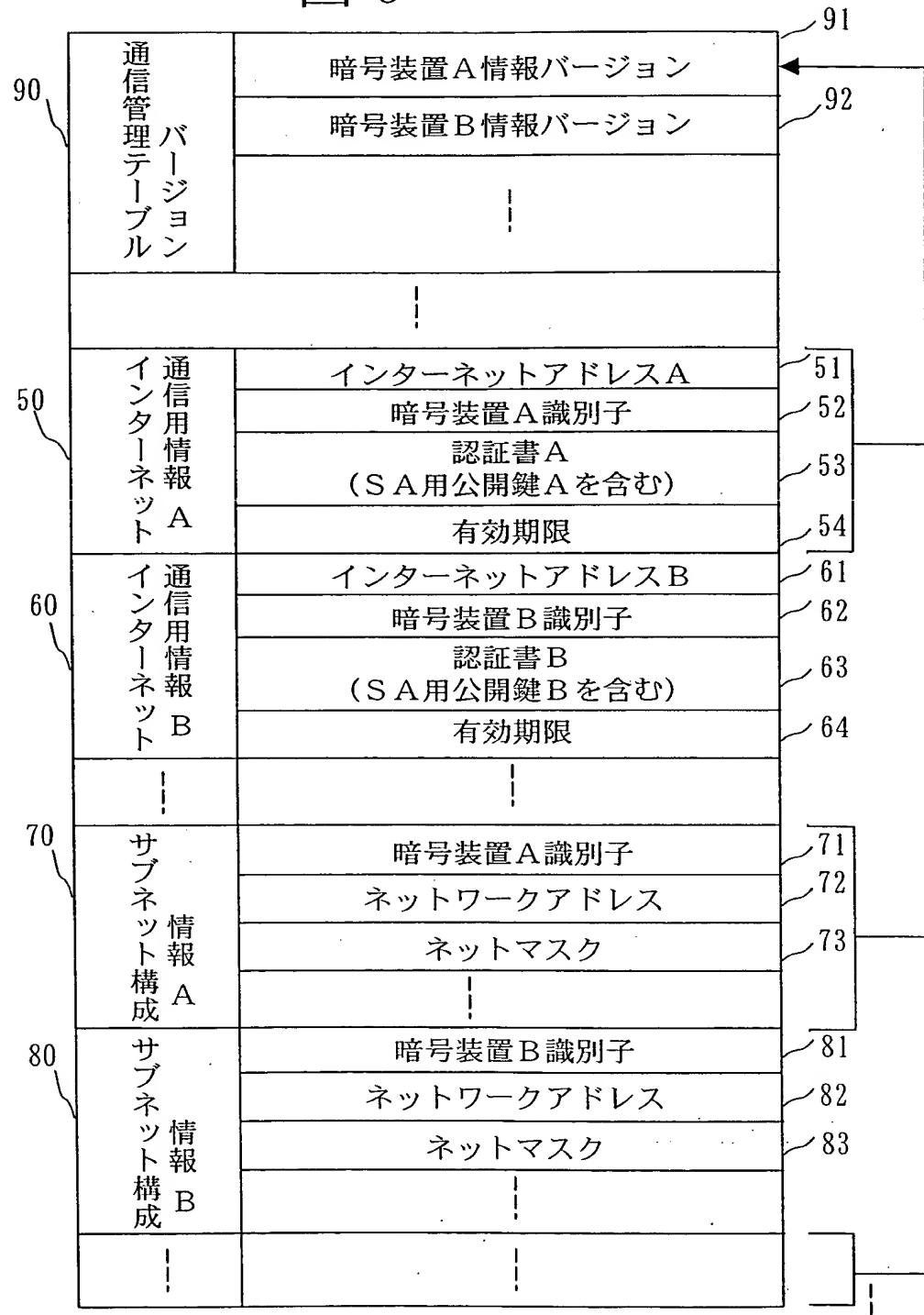
7/15

図 7



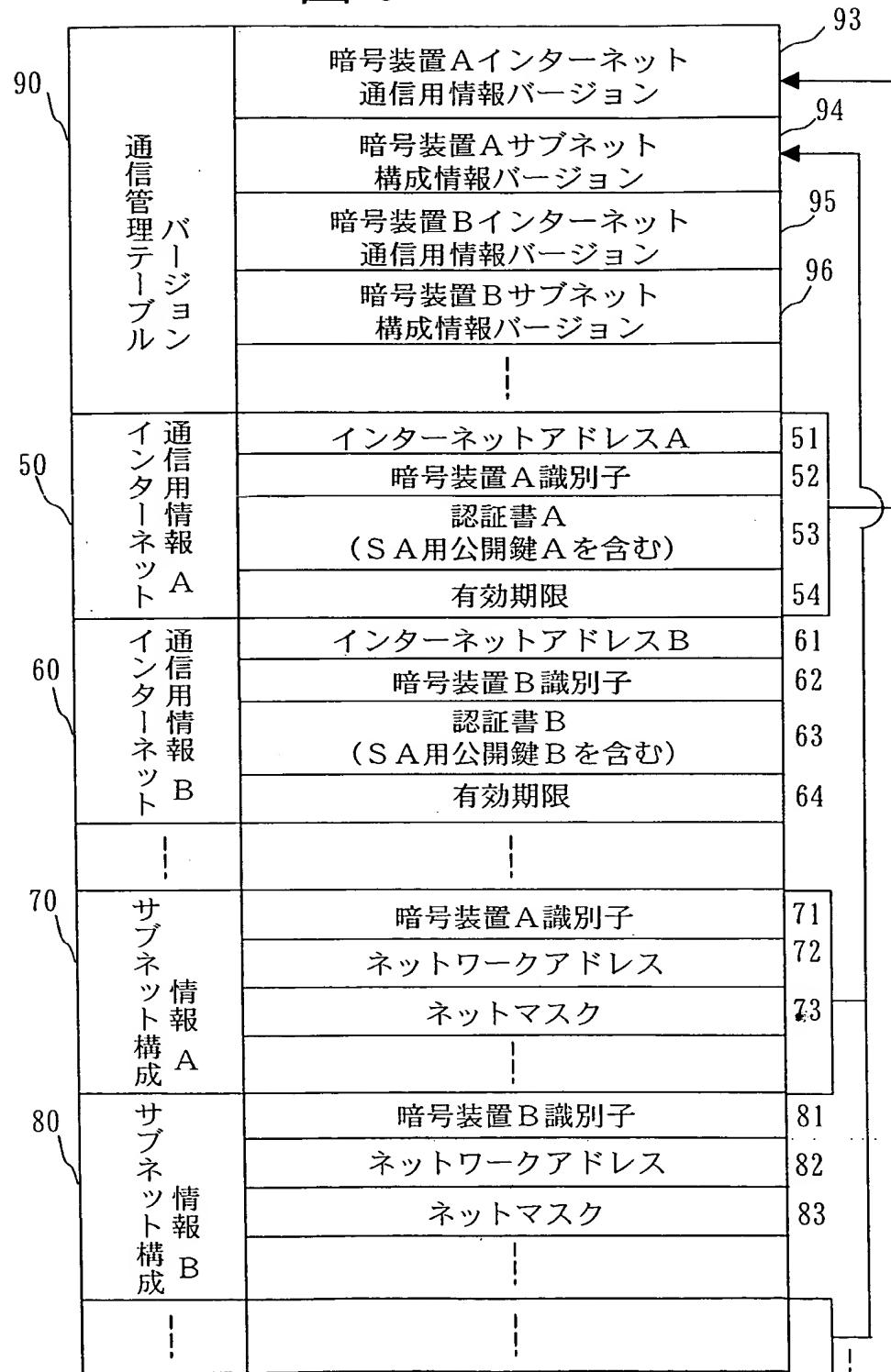
8/15

図 8



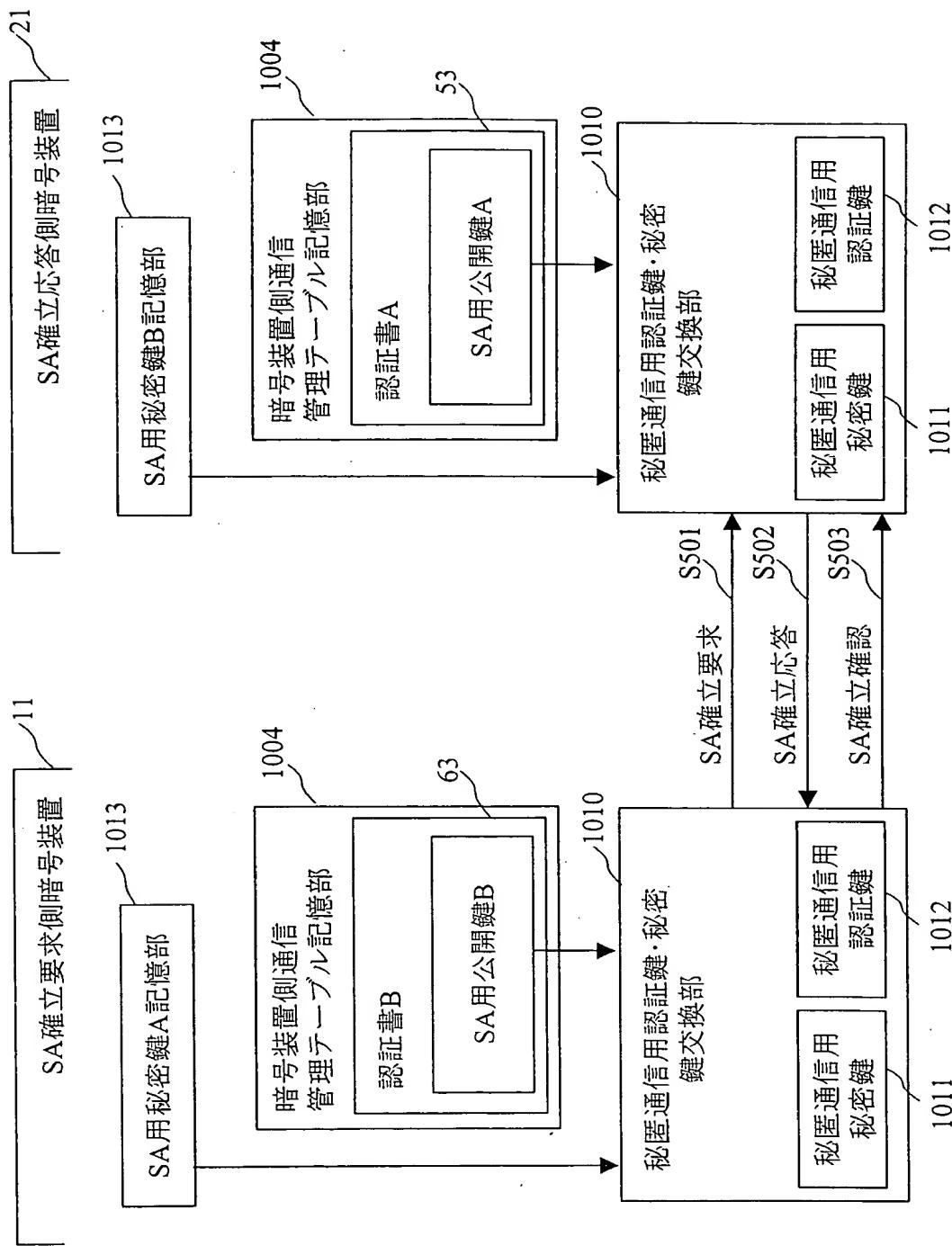
9/15

図 9



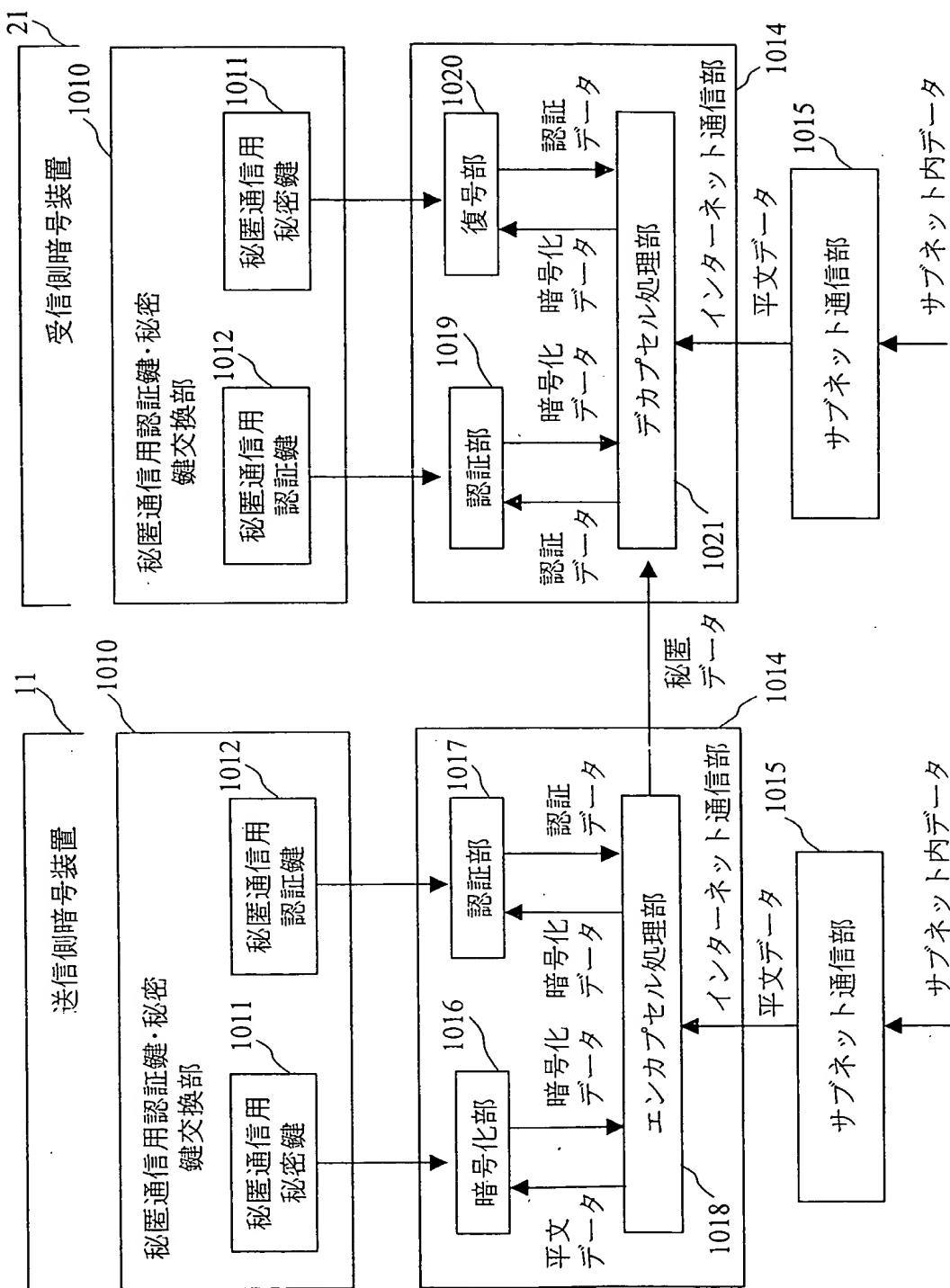
10/15

図 10

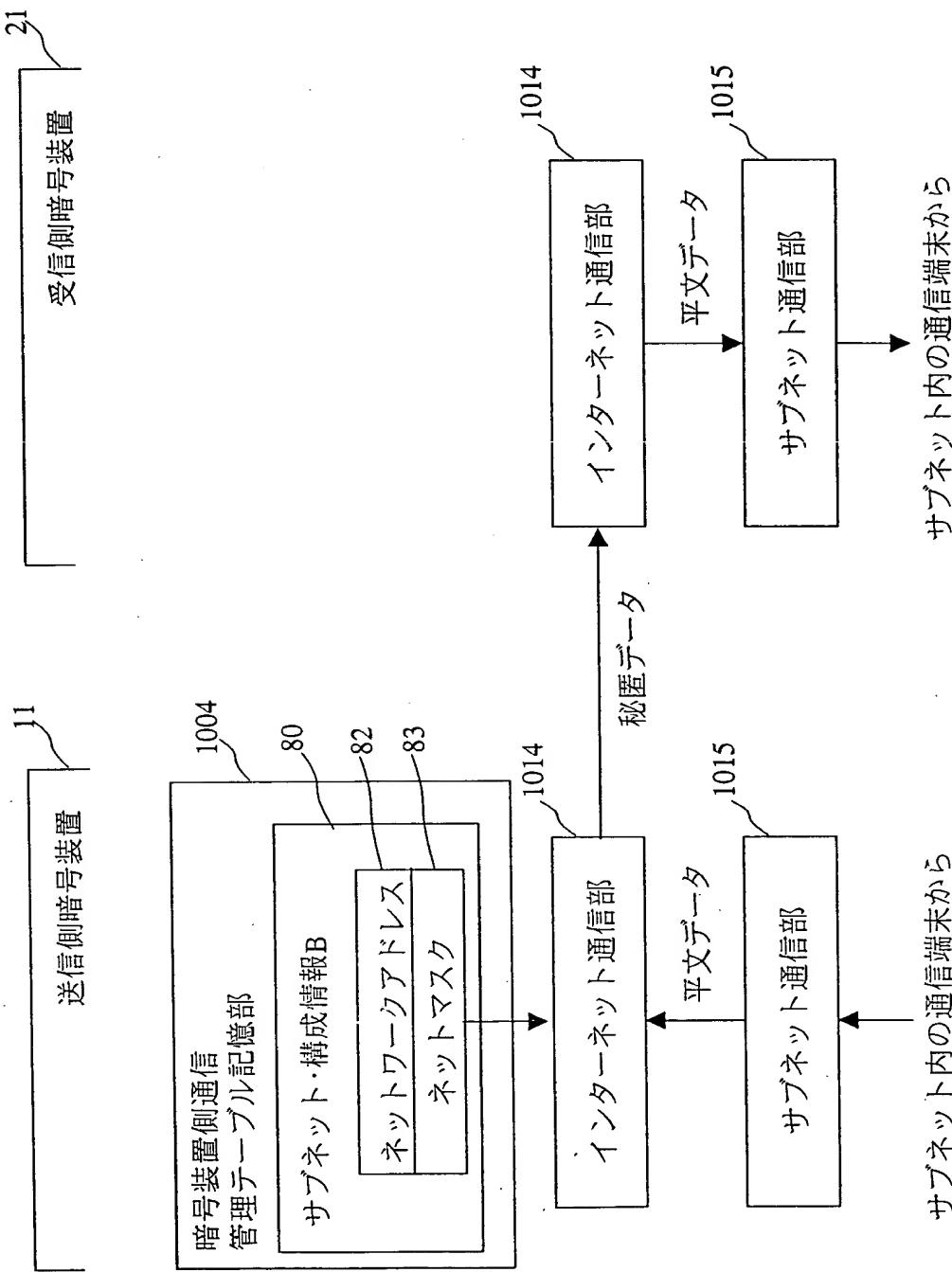


11/15

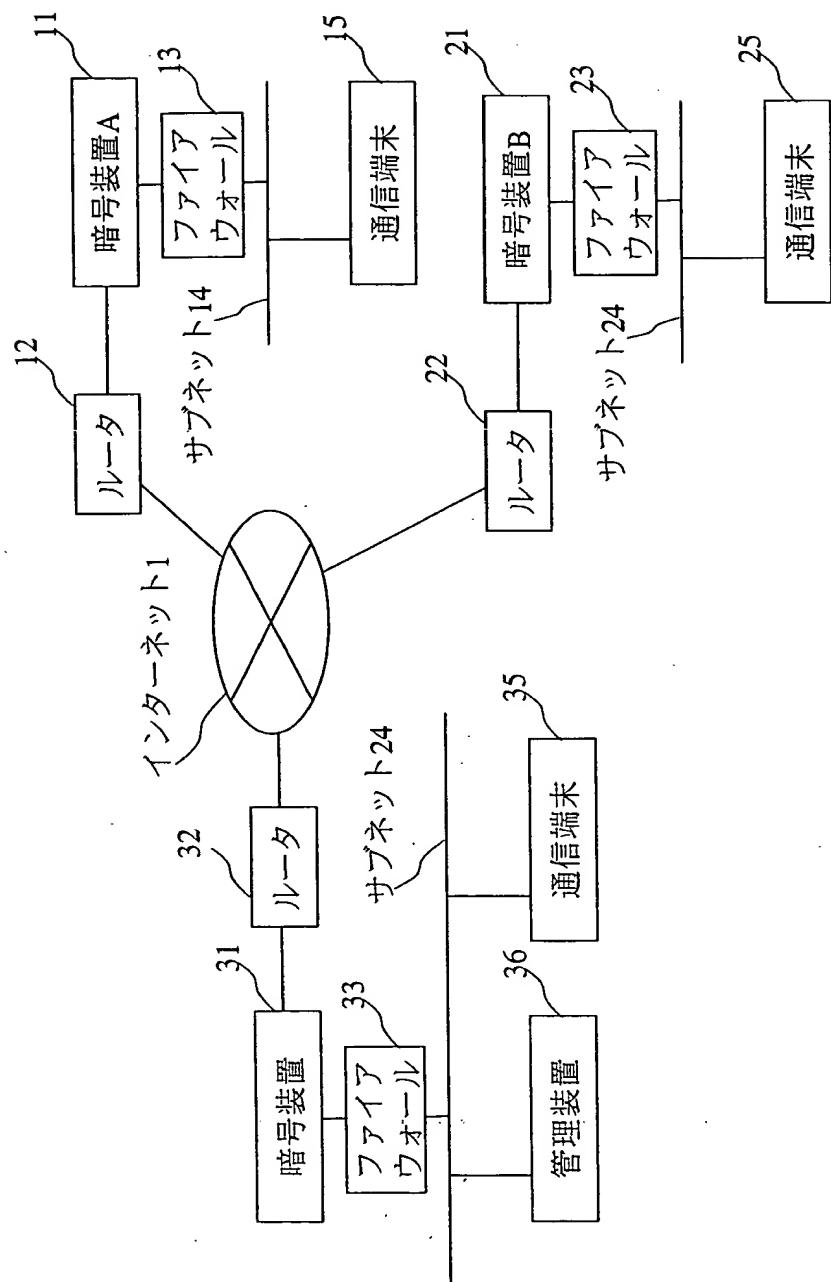
図 11



12/15
図 12



13/15
図 13



14/15
図 14

